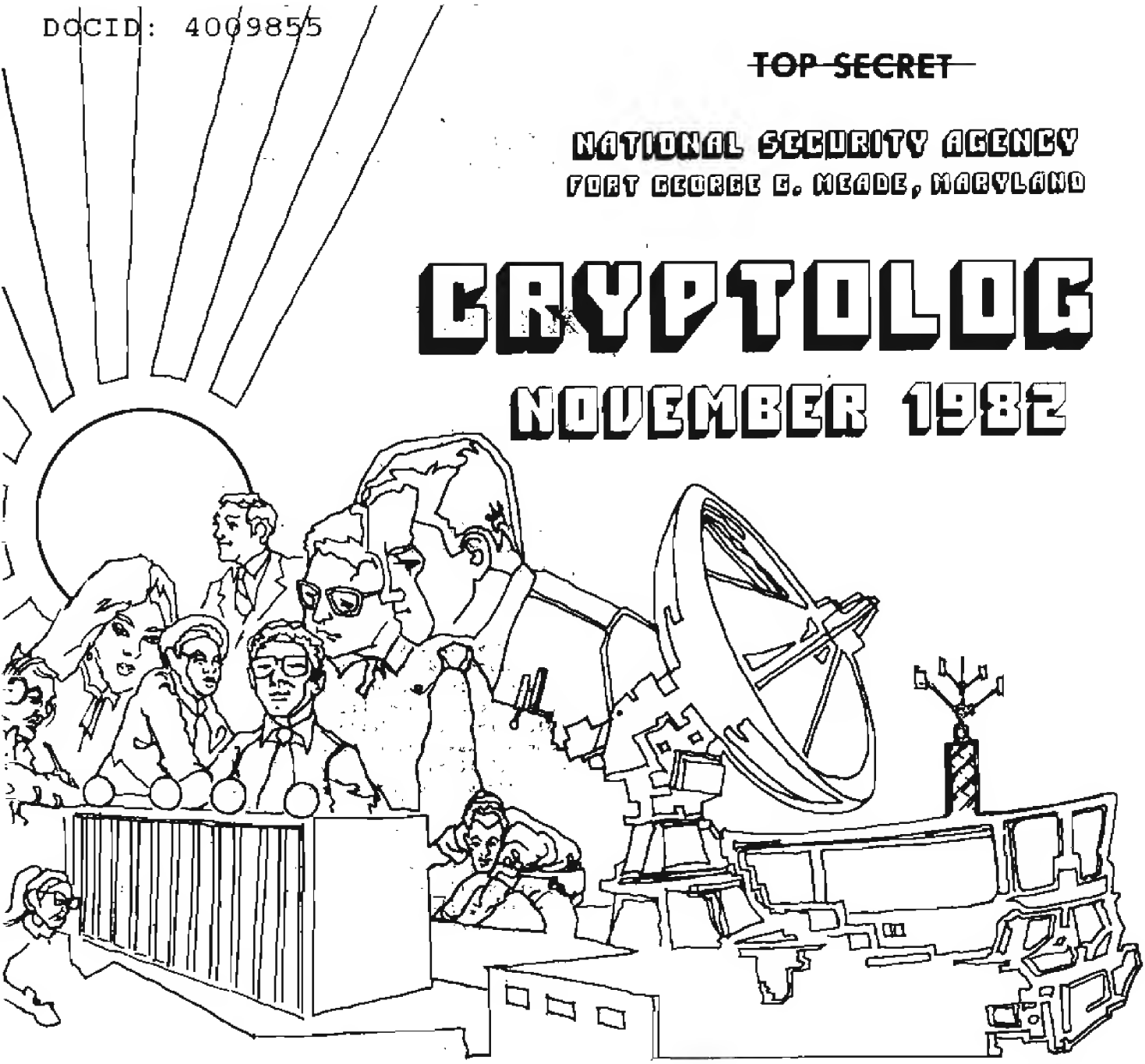
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

NOVEMBER 1982



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Not Releasable to Contractors~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 11 NOVEMBER 1982

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted] 3369s

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlc05
(bar-one-c-zero-five)
(note: no '0' in 'log')

Editorial

Some of the skill areas in the agency have no obvious counterparts in the outside world. For example, traffic analysis is not really very similar to any organized skill group in the business or academic world. (One of the old timers used to claim that traffic analysis was, in fact, quite similar to archaeology--both in techniques and age of material under study.)

Other skill areas, such as language and mathematics, do have obvious parallels in the outside world. Over the years, people in these fields have been at some pains to explain that cryptologic linguistic work, for example, was really not the same as other "outside" linguistic work. Their arguments have been persistent and persuasive.

P.L. 86-36

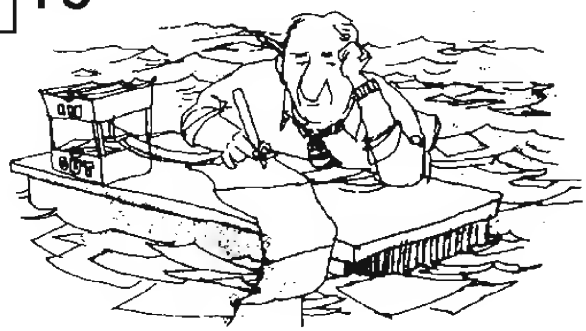
So it is rather remarkable that one of our larger skill areas, computer science, seems relatively silent on this point. At least, we do not hear the point made very often that there is anything unique about a "cryptologic computer scientist."

Perhaps the computer science people in the agency do not perceive themselves as distinct from their brethren in the outside world. Or perhaps we have not been listening to the right people.

CENTRAL RESEARCH AND THE PAPER BLOB (U)

by [redacted] T5

P.L. 86-36



(U) You've all seen it: the TV commercial in which a giant wad of paper rolls along the hallowed halls of a large company, cornering busy executives in their offices, burying them and their desks under mounds of seemingly important documents. Although this is only an advertisement, there are many at NSA who can readily identify with the situation, perhaps none more easily than those who grapple daily with the processing of this paper blob in T5, Information Resources Management.

MYTHS AND FUNCTIONS

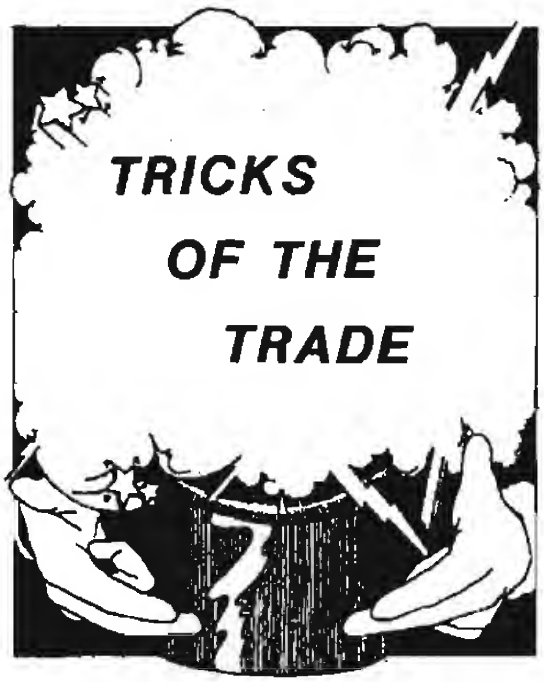
~~(POUO)~~ In particular, Central Research (T5211) is responsible for maintaining and consulting a plethora of information to ensure that the proper people somehow receive the correct information at the right moment and within a reasonable period of time. Central Research is tasked with using whatever sources are available to respond to requests from any person in any element in the Agency (and sometimes beyond) as quickly as possible. T5211 receives approximately 50 to 75 questions per day, handled by 11 full-time researchers. Queries range from the specific to the ultra-vague, from the sublime to the ridiculous. So, when some refer to Central Research as "the place where they find needles in haystacks," they couldn't be more correct.

(U) The team of experienced researchers who comprise Central Research (the old "C-Ref") are not, contrary to popular belief, "little old ladies in tennis shoes." Neither are these researchers part of the T51 Main Library, although physically located adjacent to its special book collection to share resources.

(U) The T5211 branch, besides performing research, also processes all-source (classified and unclassified, controlled and open-source) information for inclusion in automated and hardcopy information files. These 15 information specialists include analysts, technicians, and analytic aides. Most have earned college degrees, some offer foreign-language proficiencies or even translating experience, others are data base experts, two are graduates of the Information Science Intern program, and many provide invaluable knowledge acquired only through years of experience.

THE OTHER GLUT

(U) As the information explosion (or "information glut," as some prefer to call it) continues to grow, so does the rate at which new tools are designed to manage this information. It is the responsibility of Central Research and its staff to keep pace with the technology that attempts to keep pace with the information glut. This includes periodic evaluation and reevaluation of hardcopy files for possible transformation or incorporation into machine files, acquiring the relative skills necessary to effectively employ commercial and traditional search tools, and undertaking the training needed to perform as information professionals in a rapidly-changing environment.



~~(C)~~ Among the tools employed by Central Researchers in their quest for "the needle in a haystack" are:

- the reference books of the Main Library's special collection,
- government manuals and working aids,
- hardcopy files of worldwide diplomatic information,
- hardcopy collections of international organization documentation (especially the United Nations),
- worldwide treaties and conferences files,
- press clippings of current events,
- the SOLIS (SIGINT On-Line Information System) and WEEDER (State Department Cables) automated systems,
- [redacted]
- The T5 Calendar of Worldwide Holidays and Observances (prepared by T5211 and maintained on T5's UNIX-based [redacted] system),
- [redacted]
- liaison officers at other government agencies and departments,

[redacted]

This variety of sources (a Paper Blob in itself), when employed in the proper combination by those familiar with the structure and capabilities of each source, usually lead the Central Researcher to that crucial bit of information that can make or break the value of an intelligence report.

MACHINE MANIA

(U) Among all the sources listed above, the commercial data bases are probably the most talked-about and the least known-about of Central Research's tools. While some mistakenly think of them as "answer-alls," they are not. Unmistakably valuable they are. Four of these leased systems: Lockheed's DIALOG, System Development Corporation's ORBIT, Bibliographic Retrieval Service (BRS), and the New York Times Information System (NYTIS) are accessed on-line over non-secure telephone connections via commercial networks (TELENET, TYMNET, and UNINET) through a Texas Instrument (TI) 1200 baud terminal/printer.

(U) The DIALOG system alone, with its more than 150 separate files covering almost any subject imaginable, offers NSA access to more than 750,000 sources (including books, magazine articles, journals, conference papers, and non-print material). Although these files range in access fees from $10-$300 per connect-hour depending on the file, they are determined to be cost-efficient when compared with the exorbitant costs involved in scanning, processing, storing, and consulting information from those 750,000 sources.

(U) The BRS and ORBIT systems complement the DIALOG system, offering some unique files, some duplicates, and some gap-filling date ranges. These three systems provide the searcher with bibliographic information and usually an abstract (summary) of the entire article or paper. (The full text of the article or paper can then be acquired by the client through the Main Library). P.L. 86-36

(U) NYTIS, with its eight separate data bases/files, provides mostly items of news interest, especially through the Information Banks I and II and the full-text New York Times On-Line (NYTOL). Except for NYTOL, the searcher retrieves bibliographic citations to major sources. (The client can then access the full text of the article with the aid of the Main Library's personnel.) P.L. 86-36 EO 1.4.(c)

THE NEXIS CONNECTION

(U) The fifth of Central Research's commercial information data bases is produced by Mead Data Central of Ohio. Also accessed via a non-secure (but dedicated) telephone connection, NEXIS provides access to the full text of major foreign and domestic newspapers, magazines, press wires, and newsletters. Originally designed for busy executives, the system offers logical source hierarchy and can be called "user-friendly," judging by the tone of its on-line tutorials, step-by-step instructions, and brightly-colored keyboard. Beyond its full-text capabilities, NEXIS also offers KWIC (keyword-in-context) scanning, segment searches (including references to graphics), and bibliographic citations displayed on the attached CRT (cathode ray tube) screen or printed off at a 2400-baud rate.

(U) The most expensive of the five systems, NEXIS is worth its weight in gold. As Mead Data continues to add new sources to NEXIS (including APOLIT, a new Associated Press Political Service), and expand cumulative date ranges (already seven years of full text on-line for Aviation Week and Space Technology and five years of the Washington Post), the cost savings on subscriptions, time delays, processing, scanning, storing, and searching are inestimable.

OVER THE RAINBOW

(U) While Central Research and the information world expand their horizons, new applications of today's technology are considered and evaluated. Although seemingly costly at the outset, (contracts, studies, equipment, training, etc.), the long-range benefits of these new approaches to information management are actually cost-efficient and long-term. Many of these innovations can be applied directly to the commercial data bases or other automated information systems. They range from simple peripherals like CRT's, faster printers, and improved telephone communications to more complicated concepts like data downloading, on-line data base management systems (DBMS), and universal query language translators. (The typical Central Researcher today is fluent in more than 10 separate query languages!)

(U) Attaching a personal computer to the commercial data base terminals could become a reality in the near future. Many government agencies and most research organizations in the private sector already employ such technology. The implications of this advancement are many. For example, the ability to translate a multi-step logon/logoff procedure into a single keystroke on the attached personal computer saves money and alleviates analyst frustration with what can become an aggravating and time-consuming step. The ability to store queries and profiles of major interest to Agency elements and run them periodically without the usual charges incurred would also be well-worth the initial investment.

(U) Probably the single most important feature involves data downloading, or writing off search results onto an output medium of the personal computer (most likely diskettes), for storage, retrieval, and scanning later. In Central Research this could be most beneficial, as the current practice has researchers determining the usefulness of retrieved information based on their own possibly limited knowledge of a particular subject. The future sees a requestor scanning his or her own search results to determine their worth or relevance and to discover related topics.

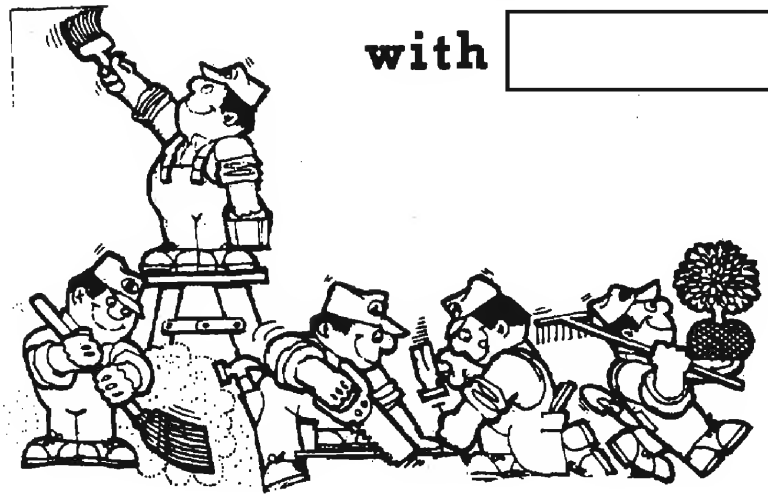
AND THE BEAT GOES ON...

(U) The list of applicable technology goes on and on. It is impossible to keep pace with all of the daily developments in this field, and unrealistic to try to "catch up" with what has already passed NSA by in the world of information management. The much-needed trend is to develop a staff of highly skilled professionals flexible enough to adjust to today's changing technology, as they take their place in a world increasingly dependent on information.

(U) In tapping all the above-mentioned resources (automated, hardcopy, and human) and by applying new technology with flexibility, Central Research can combat the Paper Blob--and win.

HUMAN FACTORS

with [redacted] **P13**



P.L. 86-36

How Do People Organize Work? (U)

We must clearly face the fact that, when we introduce a fully automated system into a set of totally manual or only partially computerized procedures, we are redesigning a large piece of people's behavior. Work takes place within an existing social grouping with a complex set of interactions, customs, and ways of relating to other people and to the jobs at hand. A whole new set of truly fascinating questions is raised for study: questions we need to know a lot more about, and which have rarely, if ever, been clearly addressed in the past. We need to go into the offices whose procedures we propose to automate and really look with open minds and eyes until we understand what the people are doing, how they coordinate and sequence their work, the way they see themselves and their jobs, and where the weak spots and strong spots are in their present procedures. The potential system users and their line managers must be involved from start to finish, and must have a decisive voice in design of the new procedures and workstations. When this approach is followed, the new system becomes "my terminal," rather than an unwelcome affliction imposed on me by the "people upstairs."

For illustrative purposes, think about your own work center in our Agency. Ask yourself the following questions, as if you were a visitor from Mars coming into the office to study the way work is done:

- When you come in in the morning, how do you know what needs to be done?
- If more than one thing needs to be done, how do you decide (or remember) which to do first?
- What about when you come back from lunch?
- What about after a two-week vacation?
- How does your boss (or how do you, if you are the boss) assign work to those on the team?
- Is it easy or hard to communicate information, advice, instructions?
- How do you go about getting information or instructions or tasking, and from whom?

Chances are that most of the answers to these kinds of questions are focused around two prominent classes of events: social (who talks to whom) and physical (presence of logs or papers or formats, location of materials in cabinets or on tables, in racks or folders or drawers or stacks, movement of materials from one location to another in a prearranged sequence). Without these procedures, there would be chaos. One of the crucial questions in office automation concerns our understanding these organizing mechanisms as they

operate in a manual or partially computerized office, and translating them sensitively and intelligently into new but functionally equivalent forms in the totally automated office.

I will use myself as an example to illustrate some of the above ideas. When I come to my work area at the start of the day, the first thing I do is to turn on my terminal. Then I get a cup of coffee and remove the black cloth from my desk, revealing a stack of folders and machine printouts I was working on the day before. They look very messy, but in fact I put them away pretty much in priority order. I usually have about three completely unconnected projects going at once. I pick up the uppermost batch of papers in the stack, look at it, and recognize it by a familiar set of scribbles, smudges, or dog-ears: "Oh, yes! That's Project X; I want to work on that this morning." I set it right beside my terminal. The second and third batches are similarly unpacked from the "mess" and positioned at slightly removed places on my terminal table: Project Y, second priority, at the rear of my table; Project Z, to be done if I have time left over, on top of my terminal. I sit down, log on, and look at my system mail if I have any. Then I call up a file whose name I remember because I assigned it mnemonically to remind me that it pertains to Project X. If I haven't worked on X for a while, and can't remember what I was doing, I may call up "XLOG", which is a journal record of my work on X for each previous day. (I keep a running log of each major project, and its name is always something starting with a mnemonic tag I assign to all files for that project and ending in "log.") Looking at the last paragraph I wrote into the file I am currently writing for Project Y reminds me of what I want to do next, and I begin keying away into my text editor window, calling up other files on a split screen from time to time as needed. SEEING WHAT I WROTE BEFORE, or SEEING A HARD COPY REFERENCE is what triggers my ideas in continuing the project, and determines my next step. In fact, I fear that I would be set back severely if my current file or log were clobbered by the system, or if my pile of papers and folders got burned up in a fire overnight!

Here is another example, drawn from a study I am making of the Agency's Payroll procedures in N41. The two-week payroll cycle is divided up into two different kinds of work: the first week is "Process Week," when time cards are collected and processed, the payrolls are balanced, and checks are issued; the second is "Variation Week," when changes are entered into the payroll records. During "Process Week" all the action is focused on the Time and Attendance Cards. They are gathered, sorted, checked against the records in the the CARILLON system, carefully scrutinized and corrected, and filed away for future reference. Since the physical time card is a legal record of employee attendance, this punched card must remain at the heart of all procedures. Procedures in the Payroll office are highly dependent on close teamwork, meticulous attention to detail, and dedicated care. Batching of the punched cards in separate piles each to be processed in a specific way is a very important part of the procedure. A large table at the front of the office serves as a work staging area, with cards and machine listings laid out in an orderly arrangement.

During "Variation Week" the focus changes to a set of documents which each payroll clerk has collected in a folder. These are official requests and notifications for changes to the employee payroll records. The clerks examine each of these documents, check the requested change against files of machine runs and previous time cards, and make changes using M204 update and retrieval segments on CARILLON. Some of the records, procedures, and determinations they must make are of astonishing complexity and require extensive research, dedicated care, and meticulous documentation. In summarizing my impression of the way the Payroll office works, I would say that everything depends on documents and cards being totally accurate and complete, and being placed in the right location (batch, folder, notebook, file drawer) at the right time.

Let's look at a third example from a very different kind of office: a transcription shop. The transcriber gets tapes to be worked on from a cabinet or drawer where they have been placed, in priority and target order, by a technician or supervisor. He logs the tapes in and out with his initials in a tape log maintained on-line in his STEPSTONE computer system. Once he has a tape, he mounts it on his recorder/reproducer, and works his way through it with the aid of a machine printout that lists the contents and may be annotated by a prescanner to indicate which segments should be transcribed and how detailed the transcript should be. His record of what he is doing consists of the tape reels he has mounted or stored in his desk, with the data about them on the jackets and accompanying printouts, notes he makes on the printouts, and the transcripts he has entered into STEPSTONE. If he stops work in the middle of a tape track, he may dismount the tape just as it is, half on one reel and half on the other, and store the reels in his desk with their rims interlocked; then he can mount them again right where he left off. The supervisor can find out who is doing what by looking at the on-line tape log. As tapes are completed, they are logged out and placed in a specific

file drawer and after they are checked they are placed in another cabinet. In this partially automated office, we can see that physical locations are still quite important. It is interesting, however, to consider what will happen if analog tapes are no longer the form in which work comes to the transcriber, and he gets his work in digital form, stored in computer files. How, then, can we help him and his supervisor keep track of where he is, and of who is doing what?

I suspect that one good way to understand what is going on in an office is to ask this question: What are the key OBJECTS around which the action seems to take place, and where do the workers go to get them?

They may be computer files, and workers may access them at CRT terminals or through listings. They may be hardcopy documents, stored in folders or drawers. They may be punched cards (as in the Payroll process) or magnetic tape reels (as in the transcription shop). In almost every office, however, we can make sense out of the seeming complexity by looking for the small set of basic kinds of OBJECTS that lie at the center of everyone's work.

Another key question is "How does work get organized?" How do workers find out about and keep track of what is next on the agenda?

A third key question is "How do workers coordinate their efforts?" The answers to these last two questions often also involve OBJECTS and LOCATIONS--logs, folders, counters, tables, piles, duty rosters, etc.--as well as meetings, discussions, and other less formal mechanisms. When we attempt to automate a manual or partially automated procedure, we must be certain that we fully understand the objects and locations that are central to the work as the workers see it. If we do not preserve the essentials of these objects, locations, and relationships in the new system, the job will cease to make sense to the workers in the office, and accuracy and productivity will suffer.

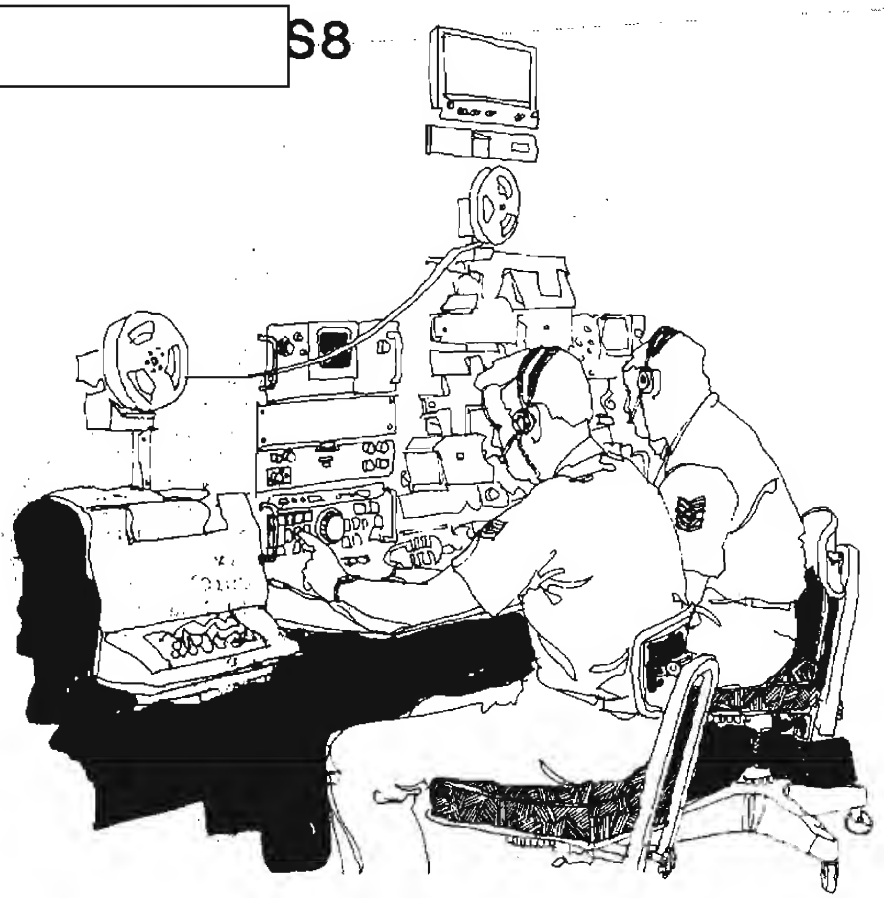
I don't want any reader to think I am arguing that office procedures should stay the same, or that the specific ways the work of an office is NOW organized must be preserved in every detail after automation. What I am urging is that we understand how the present system really works so that we can ensure that the new system includes provisions for the coordination, data flow, recordkeeping, and teamwork that the present system depends on. In fact, we should understand the present workings of our office so well that we can design a new system which will IMPROVE on the existing objects and locations that keep the office ticking. If we don't understand the present system, how can we expect to improve on it?

Up until recently, we have never really tried to automate all or most of what goes on in an office. Automation has usually consisted in running a computer program or using machine procedures to carry out scattered tasks at various points in the day's or week's work of the office. If we did a poor job of software design from a human factors point of view, it may have inconvenienced a limited set of users and degraded the performance of one set of tasks. Everything else in the office could still get done, thanks to the routine human context (procedures, habits, conventions regarding familiar OBJECTS and LOCATIONS) that we took for granted as a background to the machine procedures, and independent of them. Now, however, we are considering automating much, if not all, of what everyone in the office does, every day, week in and week out. That will involve changing the informal ways of doing things, and replacing them with automated procedures which we must design. Mistakes in human factors design will now have the potential of seriously disrupting the communication, accountability, and teamwork throughout all the work in an office. We can no longer afford to take for granted or ignore any of the activities that go on in the office and keep things running smoothly.

COMSEC CHALLENGES (U)

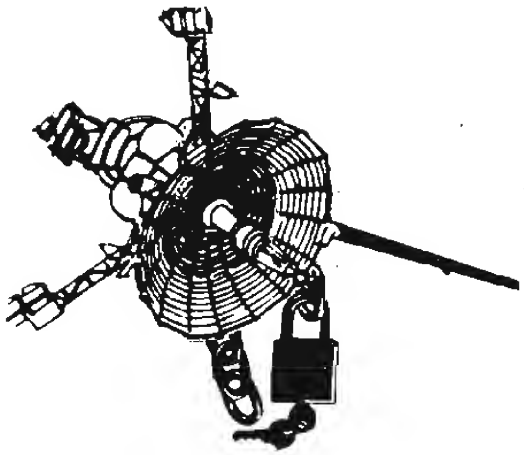
by [redacted] S8

P.L. 86-36



(U) Technology is creating new challenges to COMSEC. Microcomputers, packet-switching, growth in data terminals, etc., are stimulating new requirements and applications for which the line between communications and COMSEC is virtually nonexistent. Traditionally, COMSEC equipment has been viewed by communicators as an individual component--separate from the communications system for which it is intended to provide security. This view is changing--given today's technology. This paper provides an overview of selected technological advances within the past decade that are having a definitive impact on the way COMSEC hardware and software are designed, produced, and implemented into a data communications system.

(U) The single, most significant, recent advance in technology has unquestionably been the introduction of integrated semiconductor devices. It took several decades--through the 1950's--to optimize vacuum tube technology. At about the time that miniature vacuum tube technology was being optimized, the transistor was commercially introduced. Transistor technology was a breakthrough, but there was a lot of skepticism about the transistor's ability to replace the vacuum tube. The skeptics were proved wrong by the rapid growth and application of transistor technology. The tremendous success of the transistor seems to have led to its own self-demise; the transistor stimulated new research which, by the early 1970's, led to the commercial availability of the semiconductor "chip." The chip demonstrated that



several transistors can be simultaneously produced--each with practically identical characteristics--on a common slab of silicon about one square centimeter in size. During the 1970's the chip's silicon real estate became priceless. New manufacturing processes permitted the production of chips with the equivalent of hundreds of transistors. This large scale integrated (LSI) technology evolved into very large scale integrated (VLSI) technology (10,000 transistors) and we will soon see chips with the equivalent of 100,000 transistors.

(C) Because of their high reliability, low power consumption, and low cost, integrated circuits (ICs) have become readily available and have resulted in a phenomenal growth in data communications while creating numerous challenges for the COMSEC community. Following is a discussion of some specific and very direct results that the chip and its impact on communications technology are having on COMSEC.

(C) Many government agencies provide a data communications service that includes a variety of remote terminals in various locations that are engaged in interactive time-shared dialogues with a host computer. In certain facilities, a remote terminal on which classified work is to be performed must be located within a vaulted room. Such installations are very expensive, entail a lead time on the order of years, and require an allocation of substantial floorspace for the purpose. The electrical connections between many classified terminals and hosts is achieved via protected wireline distribution systems (PWDS); these are very costly and often difficult to implement. The above problems, currently tolerated in many government agencies, are being further aggravated by the continued growth and use of data terminals. The proliferation of data terminals, a spin-off effect of the IC, will place an increasing demand on the need for COMSEC equipment that is office-oriented. The use of COMSEC in a moderately secure office environment (as opposed to a security vault) will motivate novel approaches to the development of COMSEC; the equipment will essentially be tamperproof; it must be simple and human-engineered to facilitate its use by administrative personnel; perhaps for the first time, the physical appearance (i.e., color, size, shape) of the device will be the determining factor in its acceptance by the user.

(C) The proliferation of data communications and computer technology has resulted in telecommunications systems with many different hosts and a spectrum of terminal equipments operating at various speeds, line disciplines, interfaces, and protocols. Many of these terminals use American Standard Code for Information Exchange (ASCII); many use Extended Binary Coded Decimal Interchange Code (EBCDIC); operational speeds vary from 75 bps to 19.2 Kbps. Compounding this problem is the wide spectrum of network architectures that are used to connect terminals and hosts. For example:

- IBM's System Network Architecture (SNA) uses the character-oriented Binary Synchronous Communications (BSC) protocol;
- Digital Equipment Corporation (DEC) uses its Digital Data Communications Message Protocol (DDCMP) for all network link control;
- Advanced Data Communications Control Procedures (ADCCP) has been mandated by Federal Standard 1003 for use on government purchases of synchronous data communications equipment;
- CCITT recommendation X.25 identifies the high-level data link control (HDLC) protocol as a standard for use between a terminal and a host.

Many more examples can be cited. All of this has resulted in a COMSEC requirement to provide crypto-equipment with a high degree of flexibility so a variety of terminals can exchange data over different types of communications channels and operate with different line protocols.

(S) Currently, end-to-end security is achieved via link encryption along the transmission path and the manual processing of plaintext by cleared personnel at intermediate switching/communications centers. This concept is costly in terms of providing the intermediate personnel with system-high clearances and has the disadvantage of exposing all traffic to personnel without a "need to know." The latter has been expressed by many communicators as a serious concern with the potential for compromise and/or mishandling of classified traffic. The military departments have expressed a similar concern regarding the cost and time required to grant system-high clearances to such a large number of maintenance and operational personnel. The problem can be expected to become more critical as the need for and use of long-haul communications continues to increase. The only practical way to resolve these problems is through the implementation of end-to-end encryption. Thus, a COMSEC objective is to provide the capability to encrypt data at its source and decrypt it at the intended destination. This is a significant departure from the current use of bulk encryption on a link-by-link basis.

(S) Current and projected growth in the use of telecommunications services and equipment is creating a comparable growth in the need of COMSEC equipment. Each piece of crypto-equipment that is fielded requires the essential key management support: key generation, key distribution, and key implementation. Existing key management concepts are very manpower-intensive and depend upon a trusted distribution system as well as highly skilled personnel for implementation. Thus, existing concepts are not adequate to meet the increasing demand for key distribution and implementation. This problem is compounded when one considers end-to-end encryption in a common-user network. The latter requires a unique key between each source and destination--a nearly impossible situation with current concepts. A COMSEC objective is to provide a means to achieve automatic remote key generation, distribution, and implementation; complementary objectives are personal authentication and access control.

(S) The growth of packet-switching technology has resulted in numerous communications networks using this technology. The many advantages of packet-switching networks (speed, flexibility, economy) over classical store and forward networks clearly forecast a continuing trend toward use of packet-switching technology. Packet switching will add further impetus to the requirement for end-to-end encryption and will likely result in the need for a communications network supporting multilevel user access--two concepts that are not readily achievable with NSA's existing inventory or COMSEC equipment. In addition, packet-switching has introduced new transmission and terminal-oriented communication protocols. These protocols--Transmission Control Protocol (TCP), Internet Protocol (IP), and Terminal Handling Protocol (THP)--will become the DoD standards for packet-switched networks. There is a need to provide communications security on an end-to-end basis for packet-switched networks; a COMSEC objective is to ensure compatibility with the new DoD standard protocols for packet-switching. This is not an easy task since the standards are still evolving and, furthermore, the DoD protocols are not totally compatible with the International Standards Organization (ISO) scheme for protocol layering. This is noteworthy since, if present trends continue, the DoD standards will be at variance with the widely accepted ISO standards. The latter presents a real dilemma to the COMSEC planner and designer. Related issues are determining what levels in a hierarchical protocol scheme are optimal for performing COMSEC functions (e.g., encryption, key distribution, authentication) and to what extent the latter is considered to be classified information.

(S) In practice, most applications entail multichannel networks wherein a central computer exchanges messages and data with some number of remotely located terminals. In such configurations, with N remote terminals in operation, 2N key generators are required (one at each end of each link). This situation results in a large number of key generators at the host computer location with a corresponding increase in the probability of failure, high cost, more power consumption, floorspace, etc. The situation will worsen as the demand for data communications services increases. There is a COMSEC requirement to provide time-division multiplexing of the COMSEC functions over N input/output channels such that N remote terminals can securely interact with a central computer, thereby requiring only N+1 key generators. The cryptoconcentrator must be capable of providing link or end-to-end encryption and must be compatible with packet-switched networks.

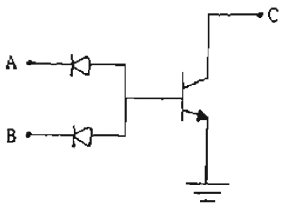
(S) The use of microprocessors and microcomputers in crypto-equipment is becoming pervasive. In addition to control and I/O functions, microcomputers are now being implemented in crypto-equipments to perform the actual data encryption. This use of microcomputers is referred to as "software encryption." Software encryption is vastly easier to implement than classical hardware encryption. Although slower in throughput speed, it

is also vastly cheaper. A typical eight-bit microcomputer can be purchased, in quantities, for less than $5.00 each. A computer programmer can program the PHALANX algorithm in a few hours. It would be impossible to accomplish the same in hardware using discrete components. There are definite benefits to software encryption; however, there is also the potential for serious risk. Consider the following software-versus-hardware approaches to achieving a simple, logical "OR" function.

- The hardware approach consists of discrete components--two diodes and a transistor--that are tangible.

- The software approach consists of some lines of code written by a programmer and executed by the microcomputer to achieve the same end result.

Logical OR Operation
C=A+B

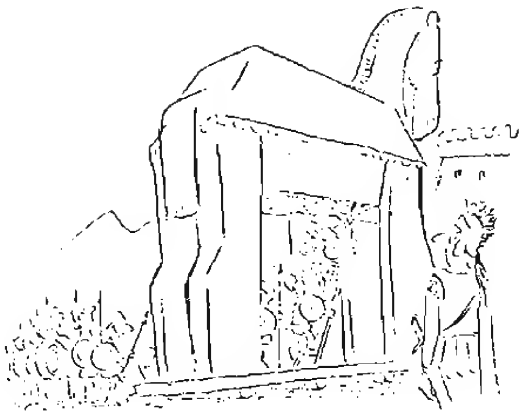


(a) hardware implementation

```
L  R1,  A
L  R2,  B

OR R1, R2
ST R1,  C
```

(b) software implementation



(S) The hardware "OR" is physically real and hence easily evaluated; the software "OR", although functionally identical to the hardware "OR", cannot be empirically evaluated--at least not on a component basis as the hardware "OR" can. This situation has created serious concern (in particular, the Trojan horse attack[1]) and is changing the way COMSEC is being evaluated. The duplication of all crypto "chip" hardware and software is often required as a means to detect failures and programming errors; to alleviate the probability of a Trojan horse, it has been recommended that COMSEC contractors be selectively required to submit to polygraph testing.

(S) As stated above, the use of micros in crypto-equipment extends beyond the encryption function. The I/O features of a key generator are greatly enhanced through the application of microprocessors. Microprocessors and/or microcomputers may be used in a key generator to accomplish a multitude of communications functions:

- TDM multiplexing
- protocol conversion;
- peripheral interfacing:
- modulation/demodulation;
- speed conversion, etc.

As a result of their availability, low cost, and ease of implementation, there is a growing tendency to employ microcomputers to couple many communications requirements with COMSEC requirements. This concept is received quite favorably by COMSEC users although it raises an institutional question within NSA: How far

does NSA go (i.e., where is the line drawn between communications and COMSEC)? Two things seem clear; first, the concept of coupling selected communications functions with COMSEC is beneficial, from a system engineering standpoint, to the COMSEC user as well as to NSA; second, NSA will inevitably be satisfying more communications functions than in the past.

(S) Cryptography in the user's terminal is an area that will receive close scrutiny in the near future. As the cost of data terminals decreases, new applications will continue to surface. The low cost, convenience, and operational efficiencies associated with the use of data terminals will bear similar demands on the COMSEC required to secure these terminals. Future COMSEC will be subject to the constraints of the office environment and, hence, there will be a natural tendency to make the COMSEC transparent to both the user and his environment. The concept of an integrated cryptomodule (CM) is operationally attractive; however, it poses numerous challenges to the COMSEC designer and evaluator. Application of an integrated CM is sure to extend beyond data terminals. Requirements have already been identified for implementing a CM in a bus interface unit (BIU) used in local area networks.

(S) The doctrine required to support the use of COMSEC in an office environment will be critical. The wide variance in applications will make it difficult to assess the threats and vulnerabilities of each application. The extent to which tamper detection measures (e.g., QUADRANT [2]) alleviate physical security concerns has yet to be determined. In any event, COMSEC doctrine will be relied on--more in the future than in the past--to fill any uncertainty voids inherent in COMSEC hardware. Established doctrine and policy with regard to handling and use of cryptomaterial will have to be revised since electronic key generation and distribution will introduce new operational concepts and procedures. Because of the retentivity charactaristics of EPROMs (Erasable Programmable Read Only Memory), their very use in COMSEC applications has already caused serious concerns. The advent of end-to-end encryption in a common-user network will necessitate new doctrine and standards to minimize vulnerabilities associated with user authentication, access control, and trusted systems. The use of electronic ignition key devices and/or personal passwords will become standard features for future crypto-equipment. Among the most interesting challenges in the area of threat assessment is the use of public encryption. DES, now available to the casual buyer on a single chip, presents an economically attractive means of achieving communications "privacy" and compartmentation. New policies and supporting doctrine are required to define the extent to which DES may be used for privacy protection in a secure communications environment.

(S) COMSEC standards and evaluations will become increasingly oriented toward communications functions. The use of microprocessors and microcomputers in cryptosystems will necessitate new evaluation techniques. The use of software encryption is among the most significant challenges to the evaluators since the circuitry within a micro (and hence, the evaluation of that circuitry) is not accessible. The need to verify and validate software will become critical. Added emphasis will be placed on software evaluation. COMSEC will have to be evaluated not only as a cryptosystem, but to a much larger extent than at present, as an element within a communications network.

(S) The area of COMSEC applications will present major new challenges. The job of defining and interpreting user's requirements--with a wide spectrum of communications applications--will be formidable. The COMSEC user is demanding. He wants a secure device that is operationally transparent, has a multitude of communications features, a highly flexible interface capability and, as usual, low cost. These demands will have to be pursued with some sense of urgency so as to dampen any user tendency to seek "interim" solutions (e.g., DES) in lieu of high-grade cryptography. The broader task at hand is one of grasping the scope of the user's changing requirements and to coalesce these requirements with evolving COMSEC doctrine and standards. The user's acceptance criteria (operationally oriented) are different from (although not usually inconsistent with) the acceptance criteria defined by NSA which are naturally security-oriented. Both sets of criteria have to be addressed with little room for trade-offs in some cases. In the final analysis, however, it is the COMSEC user who determines the extent to which a cryptosystem will be categorized as successful.

---

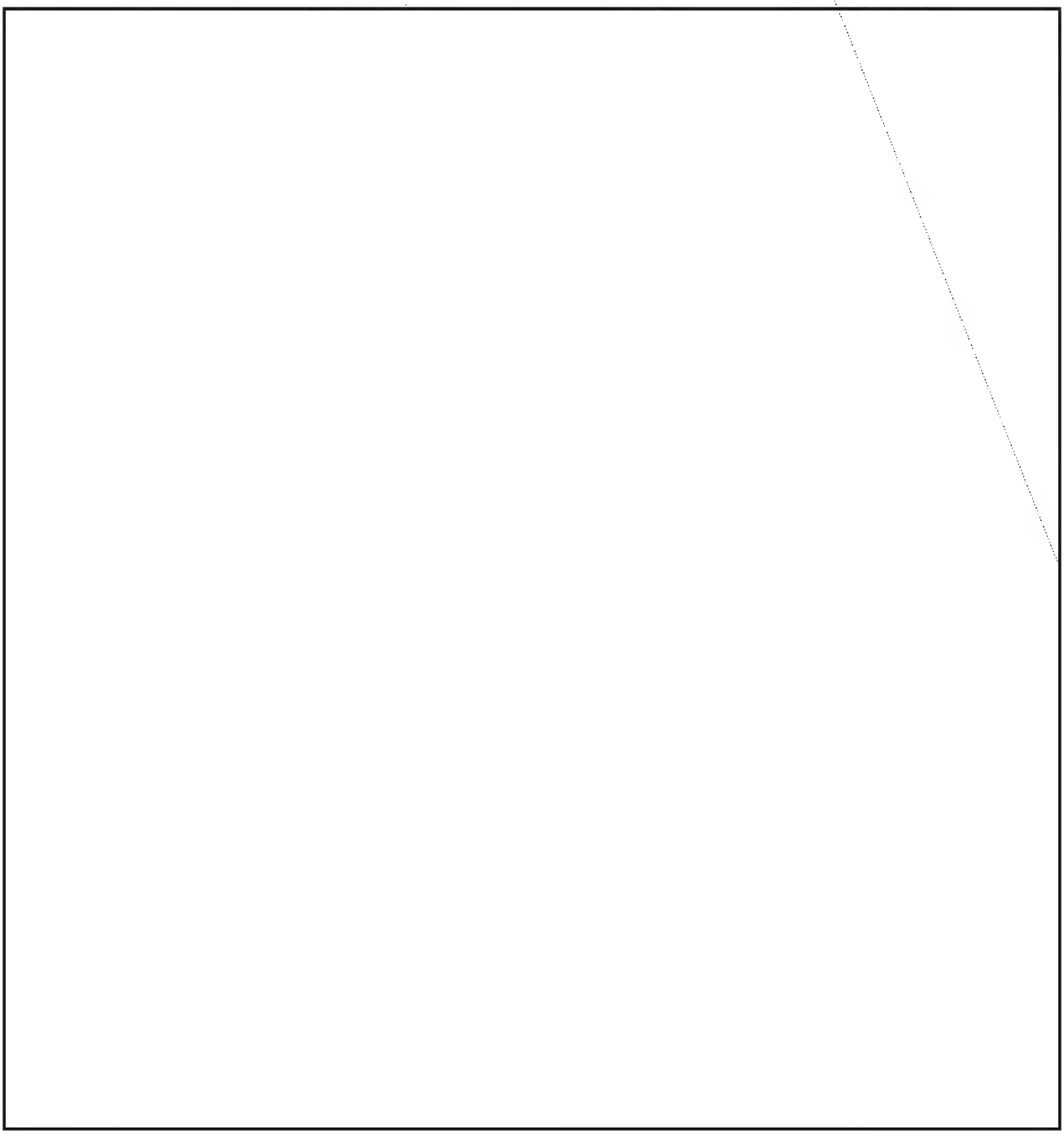
1. "Trojan horse" refers to a ploy whereby a programmer hides within a legitimate, often-used program some additional code completely unrelated to the documented function of that program. That code, for instance, might search the storage system for data to which the programmer has no access.

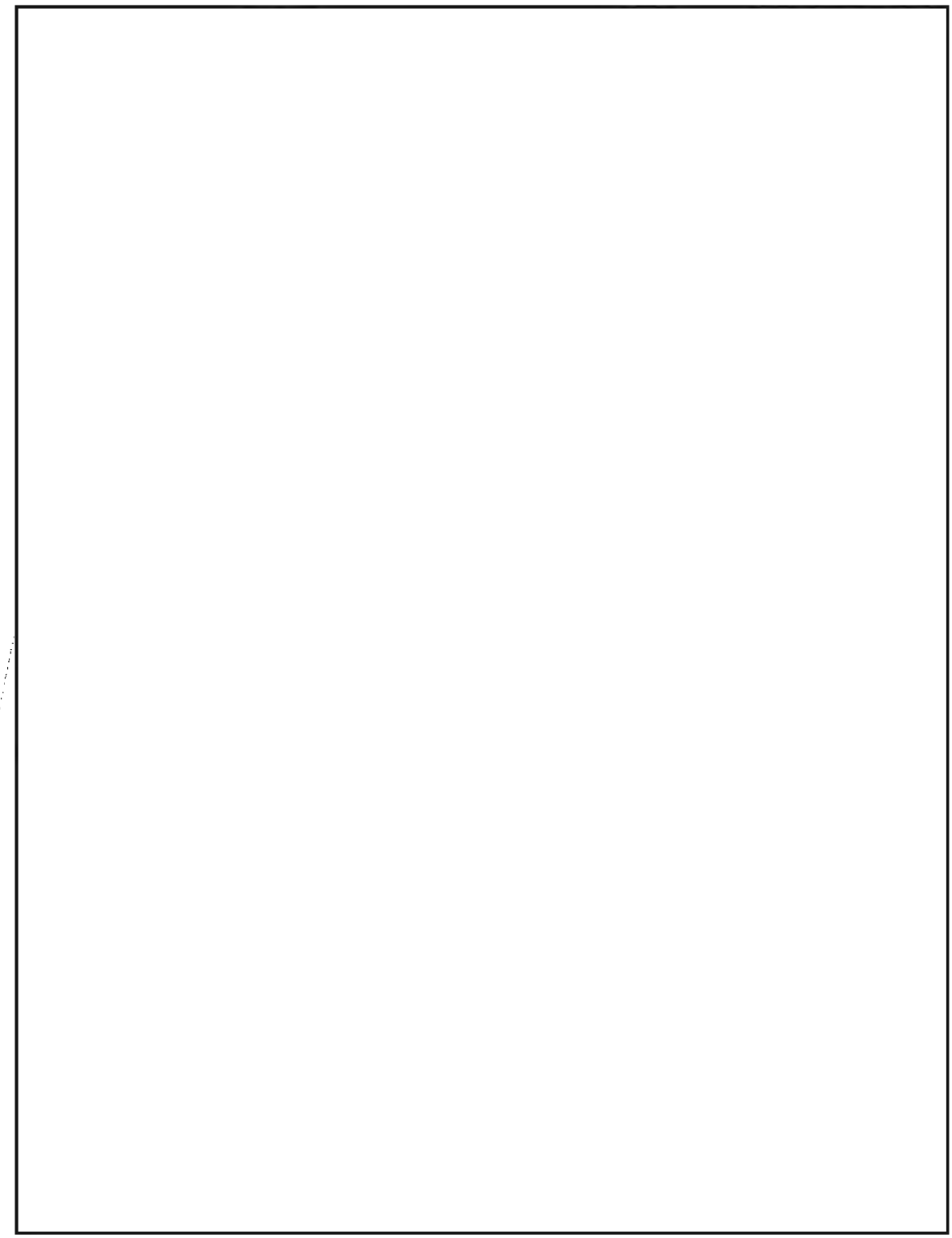
2. "QUADRANT" refers to a variety of hardware and software techniques used to detect the unauthorized tampering with a crypto-equipment.

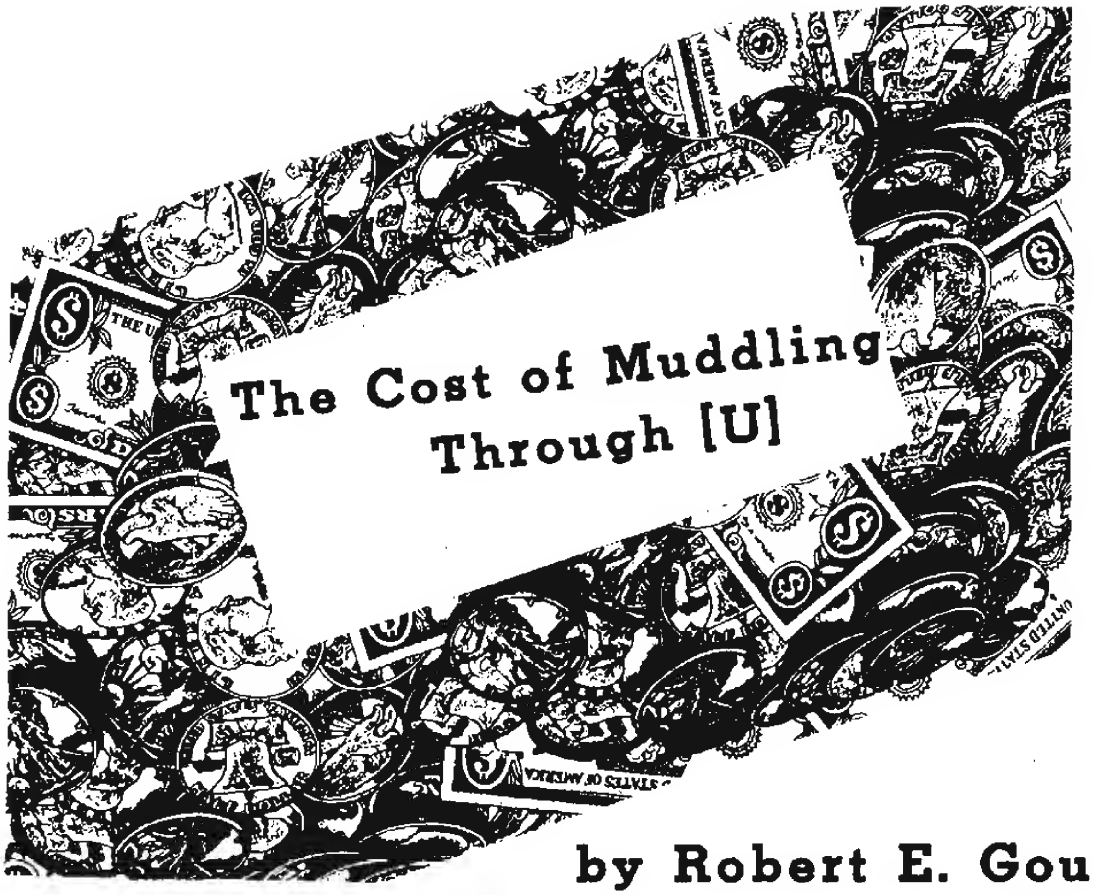
P.L. 86-36

NSA-Crostic No. 44

By D.H.W.







by Robert E. Gould

(U) In beginning this paper, I must state for the sake of clarity that I am not concerned with individual linguists so much as I am with the career of languages. The field of languages is not static but is susceptible to progress or regression. Whether or not it does progress depends upon the relatively few who can provide it leadership. It is my conviction that as it is presently constituted, the language field does tend to lose a significant number of its potentially most valuable members and does not make full use of those who remain in the field.

(U) In considering a career field or profession, attention should be given to all the factors that make up a career. When given a choice, people normally select and remain in those fields that offer money, security, prestige, individual recognition, variety of experience, and opportunity for personal growth.

(U) So far as money goes, NSA pays its linguists very well in comparison with salaries offered translators, interpreters, and teachers by other national and international organizations. Statistically it also offers a fair salary for linguists in comparison to that offered other technical fields in NSA. Job security has rarely been a factor with us.

(U) It might be stated at this point that if NSA's language needs could be met simply by producing translators, transcribers, and cryptolinguists, we probably would need to do no more than we are doing now. I don't think that our needs can be met by producing just

~~(C)~~ This article is reprinted from the November 1972 issue of the Quarterly Review for Linguists (QRL). The author was a highly respected linguist, bookbreaker, supervisor, and staff member in G Group and its predecessors. He also served as President of the Crypto-Linguistic Association (CLA) and as the founder and editor of Keyword during his Agency career, which ended with his retirement in 1973. He is now living in Tucson, Arizona, where he is doing biblical research.

the technicians described and if we want to get enough of the right kinds of people to stay in the field, one way to do it is to recognize where we have to offer more, as I shall discuss later.

(U) Prestige is a far less concrete matter than money, but generally it can be estimated by the hierarchical level at which a person's counsel is sought and by the frequency with which it is requested. In estimating the prestige that accrues to linguists, the following questions might be helpful. Do practitioners in the field participate in planning or decision making at branch, division, or office level? Are they kept aware of operational plans and programs? Are they consulted by their managers on decisions regarding their particular field or production in general? Are their professional opinions regarded as authoritative? In my experience, the answer to these questions is frequently, and within certain areas, generally negative.

(U) One reason for this situation is that a number of linguists have narrowed their view of intelligence production to the problems of language and have failed to see the relationship between their field and the rest of the Agency or to accord other operations their proper importance. In addition, only a few have ever phrased the problems of language processing in objective language that would make them accessible to nonlinguists.

(U) These comments are not made to belittle the specialist or his contribution, but to point out the result, that the nonlinguist manager may often regard linguists as narrow, impractical people and feel that even in the management of language problems, he can more safely rely on the advice of common-sense people outside the field. What is often hardest for the linguist to bear is that the intelligence analyst, too, may come to feel that in substantive questions, his opinion on the meanings of a text is more likely to be correct than is that of the person who translated it.

(U) There is no quick way of insuring the field prestige, but it can acquire it if the practitioners develop a wider view of their work, its place in SIGINT, and apply their knowledge. Specifically I would suggest the following:

- As intelligence producers, linguists should have a professional's knowledge of the intelligence field as it affects them; i.e., who their customers are, how their product is used, what requirements are, and how they are used and generated.

- They should have a thorough understanding of the support functions that linguists must perform for traffic analysts, cryptanalysts, collection, and ELINT. To be able to function properly as professionals, they must also acquire a fairly detailled understanding of various aspect of communications and cryptography.

- Linguists should also have a professional view of their own field--the linguist's various functions in production; research needs; training problems; the problems of field reporting; requirements of the Service Cryptologic Agencies' linguists.

(U) This knowledge is not something that can be instilled all at once into any given linguist, but it represents a basis for training of the professional.

~~(C)~~ For most linguists coming into production, a career seems to consist of ten years translating and ten-plus working at the checker's desk. The field does, in fact, contain a variety of jobs, but they are poorly publicized. About two thirds of the senior linguists in G Group have worked in two or more languages. Almost all have worked on a variety of problems: translation, reporting, cryptolinguistics, and others. There are, outside of production, jobs in teaching, as well as linguistic and cryptolinguistic research to which some linguists should be able to aspire. There are language staff groups in two of the G offices. Opportunities for overseas assignments exist in some areas.

~~(C)~~ The varieties of work should be made known to all beginning linguists. It would be desirable also to state the qualifications for the jobs in order to try to inspire some competition for them. Because there is no clearly enunciated public statement of the training and experience required for various positions, there is not much that an individual can do to direct his own career.

(U) The possibility of making a recognizable personal contribution seems denied the linguist to a rather considerable degree, since by the nature of much of his work, the quantity and quality of his achievements are visible only to his immediate supervisor. The room for personal contributions, however, is much greater than is at first apparent. The problem is that because of the peculiar isolation in which they have often worked, the linguists have rarely been led to think in terms of the needs of their field, where the contributions are needed. Another difficulty was posed by the fact that until recently there were few means for acquainting the rank and file with developments in the field, so that they might become aware of the needs, themselves.

(U) If a profession or career field is to advance, it must afford opportunity for innovative and exploring intellects. One of the reasons we lose linguists to management is not only that certain linguists want to get out of the field, but that their superiors see a more productive used of their talents in administration than in languages. A given linguist may be able to improve his skills so that he can do as much as two or three other employees, but his division chief may recognize that he has the vision to improve the output of the whole organization. Unless the field of languages can offer such people room for action of comparable scope in the profession, it will lose them and the progress they might bring to the field.

~~(C)~~ The cost of not providing opportunities for the creative linguist employee in his field is easy to delineate. It was long recognized that relying on experience as a teacher, we needed years to produce a good COMINT linguist, even in a well-known language such as Spanish, but an on-the-job course prepared by an expert was not developed until the mid-60's. It was also well known that continuing effort was required to keep up with contemporary language, but no serious work was undertaken until the introduction of the CAMINO Spanish Language File in 1966.

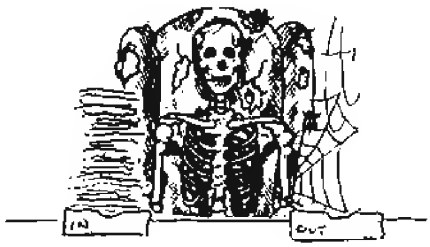
(U) The significant point of those advances is that they were made by linguists of unusual talent who had created their own jobs. If we are content to wait another twenty years for some of our other language problems to be solved, we can proceed in the accustomed manner, directing all efforts to producing desk linguists and relying on some few of them to work themselves loose at some uncertain date for work of a broader scope.

(U) The more direct approach is to recognize that we have a continuing need for inventive, practical, and broadly experienced linguists for developmental work and not only create places for them, but insure that these places offer sufficient rewards to draw the right people and keep the places filled, also with the right people.

---

1. Some specific examples recently uncovered are:

- a good, existing reference grammar requires indexing before it can be used effectively;
- specially prepared training tapes are needed for new transcribers;
- more effective means of training service transcribers may be possible by proper application of phonetic theory;
- grammars of COMINT language and usage need to be prepared in several languages;
- advanced on-the-job instruction needs to be developed in the absence of formal courses;
- more and new material needs to be assembled to expedite training of new linguists.



AN *OLD TIMER* IS ONE WHO... (U)

by W. P. Meyer, T5

Remembers when there were two Marine guards at the escalator in the middle of the Operations Building, one at the bottom of the stairs and one at the top of the second floor.

Remembers when the Headquarters Building was being built and the rumors said it was going to be reserved for all of the M organizations.

Remembers the rumor that NSA was going to be split in half, one part moving to California and the other to North Carolina, i.e., NSA East, and NSA West.

Remembers when there were so many rumors concerning anything and everything at NSA that someone said they were going to build a hotel on the Baltimore-Washington Parkway to house the "roomers," and so they built Colony 7.

Remembers when the copying machines used tulip-imprinted paper so you could tell the reproduction sheet from the original copy.

Remembers that when the IRC (Information Research Center) Building was built it was not meant for human occupancy. It was originally called the "SMSB" (Sensitive Material Storage Building). When the heat and humidity reached a certain point, everyone was excused to leave. Of course, if you were in a carpool with people from the Operations Building, you couldn't leave to go home anyway.

Remembers when a bored Marine climbed the microwave tower in front of the IRC Building one night and put up a Nazi flag, and it took the Post Engineers a week to bring it down.

Remembers when the old CREF (Central Reference) moved to the IRC Building, and no one used the library again. Every office began to build up its own collection of books. Information is so fragmented now that no one knows where anything is anymore.

Remembers when R wanted to build their own building near College Park and establish their own collection of books; here it is 20 years later and they have their own buildings, only they are called FANX-II and FANX-III, and their library is the FANX Library.

Remembers when NSA had no flagpole in front of the Operations Building. When Admiral Frost arrived, he stated that NSA was a ship and he needed to fly his personal flag so that the public would know that he was aboard.

I am not "really" an old timer. I did attend the U.S. Army Signal Corps School at Fort Monmouth, New Jersey; I did have an MOS 805 (Cryptographic Technician) but I did not start to work at NSA until 1958. A "real" old timer is one who was at NSS (Naval Security Station) or at AHS (Arlington Hall Station), or even the old Munitions Building. You should hear the stories they can tell--and I hope they will.

SIGINT: 1990 (U)
PART 3

by [redacted] P13

P.L. 86-36

COMPUTER COMMUNICATIONS SYSTEMS

~~(S-CCO)~~ As computers become more tightly integrated into telecom nets, the central problems facing SIGINT will become what to target and how. The most useful data, from an intelligence or a SIGINT viewpoint, may be resident in the system in a computer memory, rather than passing over a communication channel. SIGINT, instead of waiting for data to be transmitted and then passively collecting and exploiting them, will have to penetrate into the nets, find what is there, and extract it.

~~(S-CCO)~~ Several points, which are obvious truisms, must be borne in mind. It is fairly easy and cheap nowadays to make a link secure. This is the COMSEC function, now virtually solved. On the other hand, it is very hard to secure a whole network against every possible attack. This is the NETSEC problem, and part of the NETSEC, viz., computer security, is actually operating as a separate organization inside NSA because it is a different problem.

~~(S-CCO)~~ Although the security role of NSA is extending from protecting channels to protecting nets, the analytic role still seems trapped in the passive posture of intercepting links rather than penetrating nets. By 1990 this will not be a viable SIGINT position.

What new problems will SIGINT have to face by 1990? What do the new trends in technology tell us about the not-so-distant future? The author has adapted this article, presented here in the third of several monthly installments, from his presentation at a January 1982 session of CA-305.

This is one of the choices that must be faced and acted on.

[redacted]

P.L. 86-36
EO 1.4.(c)

~~(S-CCO)~~ The two major effects of having computers integrated into the telecom nets are logic and storage. The computers can provide services which are logically complicated, compared with old-fashioned manned message centers which were fully burdened just to receive and pass on messages. The modern storage systems can provide economical central repositories of data. Because of economics it is still not feasible to provide immense storage capacity at the subscriber outstation, because big memories cost far more than telephones. The effect of centralizing on-line memories around computer systems leads to a lot of man-machine and machine-machine data transfers. The total amount of storage capacity that is coming into the networks as on-line memory is quite significant, and currently sums to about 1 quadrillion bytes of data which can be automatically accessed by remote requests. By 1990 over 100 quadrillion bytes of online storage are expected worldwide, under various access controls. The SIGINT task is to penetrate into this on-line storage, find out what is accessible, and extract the useful data.

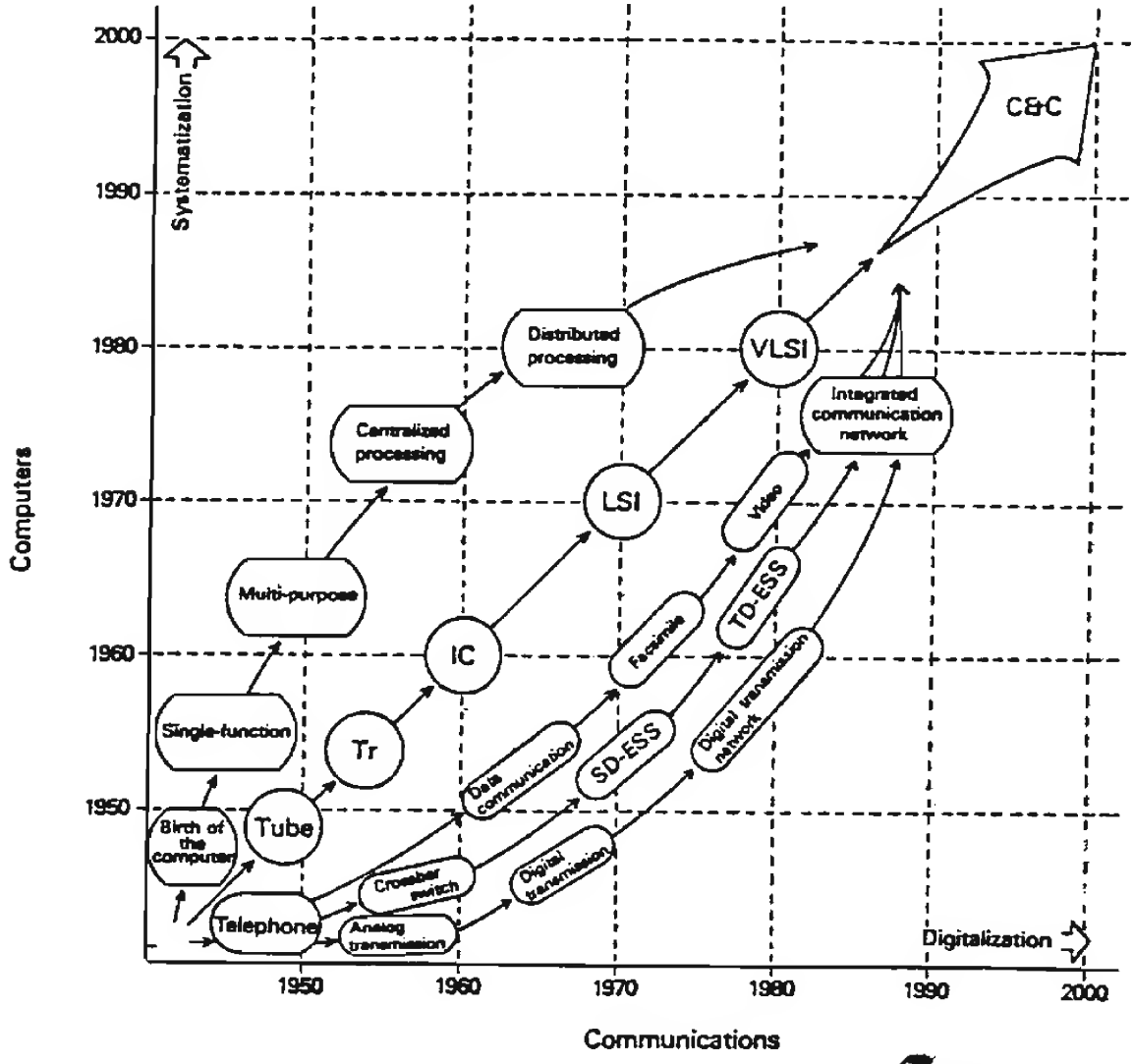
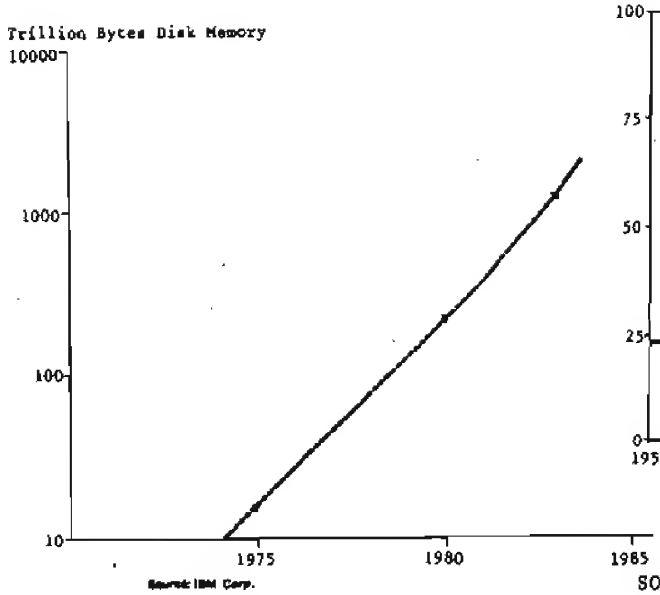


Fig. 32

PERSPECTIVE OF "C & C"



WORLDWIDE GROWTH OF
ONLINE COMPUTER STORAGE (Fig 33)

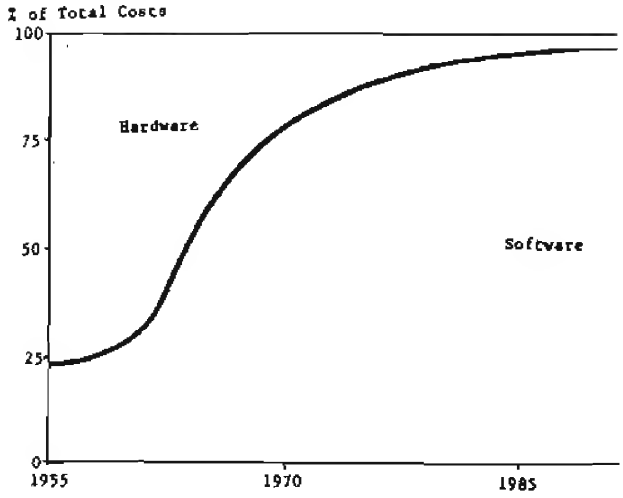
(U) Two unavoidable consequences of all this storage capacity are that:

[] first, information flow (not mere traffic flow) through the networks becomes very complicated, because data files may be located at dozens of different points as identical or slightly altered sets, and

[] second, the users are forced to think about and rely on the storage and the stored data.

(U) While a user can interact with a memoryless telecom system, e.g., a telephone net, through a mechanical terminal (telephone, teletype, facsimile), once the network has memory, especially on-line storage, the user needs elaborate protocols, embodied in software or firmware, to interpret what he wants to do into command sequences that the network can execute.

(U) The result is that in a C&C net the bulk of the investment shifts from the central switch and outside plant, which connects $10 telephones, to a huge investment in software and "intelligent" terminals which perform many different functions for the network users. Typically, 90 percent of the customer's investment is in the terminal, and the aggregate cost of producing software or firmware that the customers will purchase becomes the dominant factor in system cost and success.



SOFTWARE COSTS FOR SYSTEM DEVELOPERS (Fig 34)

(U) The performance requirements for the terminal software are not all trivial, because banking and financial services will be supplied more and more through terminals which not only give access to cash, but to many other banking services, from private or public locations. The software, firmware, and cryptography needed to assure reliable functioning will be critical.

(U) As an example, the major U.S. banks will soon be offering interstate banking services via terminals, and extension to international services is only a matter of time. Hence, critical economic information, generated by network terminals, will flow through public C&C networks, replacing much of the mail and conventional financial, shopping, and business activities.

~~(S-CCO)~~ As circuit technology has improved, software development has become the dominant factor in system cost and delivery (and performance). This software development burden will have the effect of "freezing" the network services to a considerable degree, even if the hardware is easily replaced, because of the "learning cost" that the users have to pay to get access to the system. At the same time, the burden of producing software will tend to freeze SIGINT methods, for the same reasons.

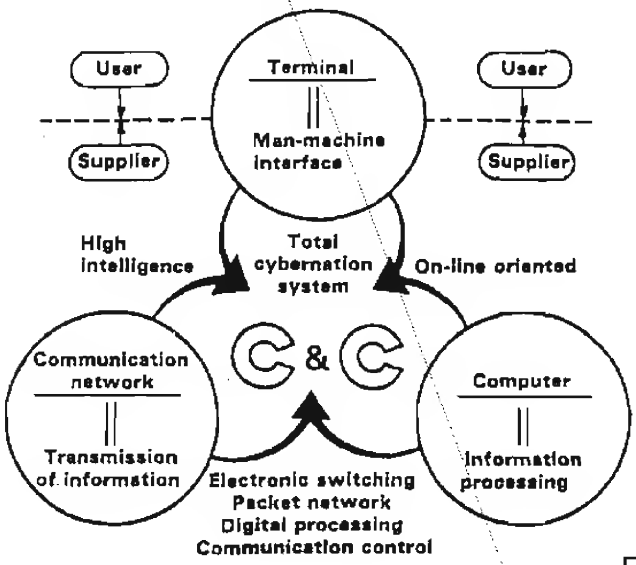


IMAGE OF C&C INTERACTION (Fig 35)

(U) A C&C network consists of a number of components, viz., computers, on-line storage, telecom circuits, switching, software, data bases, terminals, users, and projects or activities that use the C&C net.

(U) Over the next ten years the main effort in the industrial nations will be to establish the IDN (integrated digital network) as an operating entity. The object of IDN is digitalization of the local network and terminals in the form of a 4-wire digital circuit. When this is achieved, many new services can be provided, leading to the ISDN (Integrated Services Digital Network) based on 64-Kbps circuits all through the network. This will allow the C&C terminals to provide point-to-point switched encrypted voice, data, and facsimile with many data base services, and interface into other message services, such as Telex, Teletex, etc.

~~(TS-CCO)~~ The deliberate deregulation of the U.S. telecom market and the increasing role of computers and software and microprocessor terminals will tend to force experimentation and innovation onto the PTT's in both industrial and Third World countries, as powerful customers demand the procurement and introduction of useful and sophisticated new services, such as domsats, POS terminals, E-Mail, electronic banking, etc. A major advantage that U.S. suppliers have in C&C competition is the highly knowledgeable customer base that demands everything the technology can supply. The increasing internationalization of U.S. business will inevitably hurry the spread and export of the advanced C&C services and technology into all areas of the world where those companies operate. Many sophisticated foreign business C&C nets will be SIGINT targets, wherever they extend, and therefore the current backward state of a poor country's telecom plant is not a guarantee that they will not superimpose the most advanced C&C nets on top of the local plant, in the same way that inefficient subsidized jet airlines are superimposed as status symbols over oxcart economies.

COMPLEXITY OF TELECOMMUNICATIONS

(U) A century ago telecommunications consisted of Morse telegraphy. In the latter part of the 19th century telephony was added, after some initial resistance by the Post and Telegraph authorities. At the turn of the century coastal radio telegraphy was introduced and gradually brought into the network of services, although for some years the British Post Office, for example, would not allow the Marconi stations to have telephone or telegraph lines, since radio threatened their monopoly.

(U) Gradually new services were added, many based on radio, to take care of special needs such as safety services, mobile radio, marine and aircraft traffic, air traffic control, amateur, radar, broadcasting, TV transmission, facsimile, and so on.

(U) Now the capabilities of digital networks, with computers to carry out the details of providing user interface and networks access, have encouraged many new notions about what telecommunications are, and what role they should play in a modern nation.

(U) The French CNET study for the year 2000 has formulated a large number of new services which can be integrated into the future networks. A table of 64 new services has been published in the study.

Telecommunications by 2000 — Some services for the year 2000

Fig. 36 - 64 additional new services

TELE-ENERGY Monitoring & control of energy consumption	EUROPHONE Handset H/T on a Europe-wide level	UNIVERSAL IDENT BADGE An electronic passkey (also see below)	TELEFINGERPRINT Enter without knocking, thanks to voice recognition	TELEWORK Shiftwork in your home (Cf. HOUSEWORK)	TELELIBRARY Look at books, documents, newspapers, etc.	TELECONFERENCE Color, hi-fi, graphics, on a Europewide level	TELEMAIL Telecopying of the future
2-1/2D IMAGES For those who want to change their point of view	TELEHELP Pinpointing of dangerous situations	TELECONTROL Location of individuals	TELEDESIGN The Office of R&D in era of TV automation	"SLY BISON" Videotex version that can be used in a car	WEATHERCULTURE Weather forecasting in the service of agriculture	TELEFILING To save paper ...& space. (Cf. TELELIBRARY)	TELECHECKING Electronic pay cards
TELEANALYSIS Detection of pollution & toxic products	VOICE PLACEMENT OF ORDERS No more dialing; forget the keyboard!	TELEDIAGNOSTIC In case the electronic housekeeper breaks down	TELESIMULTANEOUS TRANSLATION For better understanding between people	HOUSEWORK With videomatic assistance (Cf. TELEWORK)	TELEHEALTH Computerized preventive medicine	TELESURVEILLANCE Videosurveillance for various purposes: family, social, business ...	TELEWARNING National net for detecting & warning about disasters
3D TELEMOLDING 3-dimensional facsimile	TELEARDMATION A companion, a babysitter, the life of the party	QUICK CALLS A guarantee of short duration	TELECOMPUTERS All the computers in the world want to lend you a hand	TELEVILLAGE A real estate office	IGB or IMB Individual Genetic (or Medical) Badge	TELEINFORMATION TELEADVICE Starting with data banks or a group of experts	TELETEACHING Education marches on
TELECLEANING Automatic housecleaning w/centralized supervision	TELESEARCH For doing research & paging people	TELEJUKEBOX Songs & music on the phone, w/a TELE/HI-FI version	TELESCRIPTING For the handicapped, converts the written word to Braille	TELETAXI Automated location of vehicles	TELEWEATHER A real-time service	AUTOMATIC RECALL There's this phone number that you've called (over & over)	AUTOMATIC FILTERING Freedom from the telephone
TELEDECORATING A new kinetic & musical art in your home	TELEMAINTENANCE Remote repairs. System connected to TELEDIAGNOSTIC	TELEVOTING Electronic democracy	TELEAVAILABILITY To be called or recalled when wanted	TELESTOCKMARKET Automated trading & data (Cf. TELEMART ADS & TELESWAP)	TELEPROGRAMS Bidding on TV programs	TELEMART ADS Videotex want ads (Cf. TELESTOCKMARKET & TELESWAP)	TELERESERVATION For shows, hotels, travel, w/automatic payment
TELECOUPLE Marriage by TV technology. A form of Computer-Assisted Design	TELEOPTIMIZING It will solve all your problems	TELEPOLLING See the box above	TELESOFTWARE To plug your pocket calculator into the network	TELEPRICE LIST for HCRPS Wholesalers National Computerized Retail Price Service	TELEFORUM Meetings & debates over the phone	TELESWAP A second-hand store in connection with TELEMART ADS	TEACHING TERMINAL You'll learn how to use all the other terminals
TELEGAMES Interactive video games for one or more persons	TELECOMMAND A generalization of the automatic wake-up call	INTERNETWORK Don't send anything but flowers...	TELEFLEA MARKET A teleautomated second-hand shop, employment agency, etc.	TOM-TOM Your dialing time shortened, using a card	AUTOMATIC PCV Just what its name says (PCV = Reverse the charges)	TELESHOPPING Videodiscatalogue & automatic shopping by phone	TELEAUTOMAT Away from all those fareway counters

CNET: NEW TELECOMMUNICATIONS SERVICES IN 2000 (Fig 36)

(U) This tabulation expresses the significant increase in the complexity of future telecommunications. Even marriage by telecommunications (see TELECOUPLE) is included in the plan. There is so far no mention of telenuptials. The different services interact to some extent. Some teleservices will be forced onto the user, e.g., by the banks eliminating paper checks, or by the existing French plan to eliminate the telephone books throughout France in favor of small text terminals which a telephone subscriber will use to request directory service. As the teleservices extend farther through the society and economy, the PTT's will have a much greater policy role in determining what transactions will occur in a nation. The recent telephone cutoff in Poland and in the USSR, to enforce government control, illustrates the importance attached to controlling teleservices.

[redacted]

~~(C-CCO)~~ SIGINT is familiar with the conventional point-to-point communications and with point-to-mass (broadcast) nets, but computers now make mass-to-point nets feasible, which collect data or serve a star net of subscribers.

(U) Different parts of the networks will grow at different rates; e.g., in Japan computer production has grown at 20 percent, while video tape recorder and robot production have grown at almost 50 percent. Facsimile, word processing and other office information equipment have grown at 40 percent.

(U) Both government and business, through teleservices, will be able to reach out through the telecom nets and extend an interactive environment over time and distance. The teleservices may extend from the exercise of police or taxing power to the marketing of luxuries. Ownership of the teleservices will be important, just as ownership of the telecom plant also confers power. As competitive nets, offering similar teleservices, extend further, there will be greater emphasis on controlling the flow of information within and between nets. Encryption will be only one of the means used to control or regulate access and flow.

(U) Although the French model projects the future in terms of different services, a rather different view of current telecommunications and media was presented in recent Congressional hearings about competition in the communications industry.

THE MEDIA BUSINESS, 1981 (Fig 37)

(U) The tabulation in the hearing record, which was adapted from a Harvard study, roughly segregated the broadcast services from the various means of delivering information. The resulting somewhat crowded and inscrutable chart is a testament to the difficulty of describing the conglomerate of products, services, channels and content that constitute modern communications.

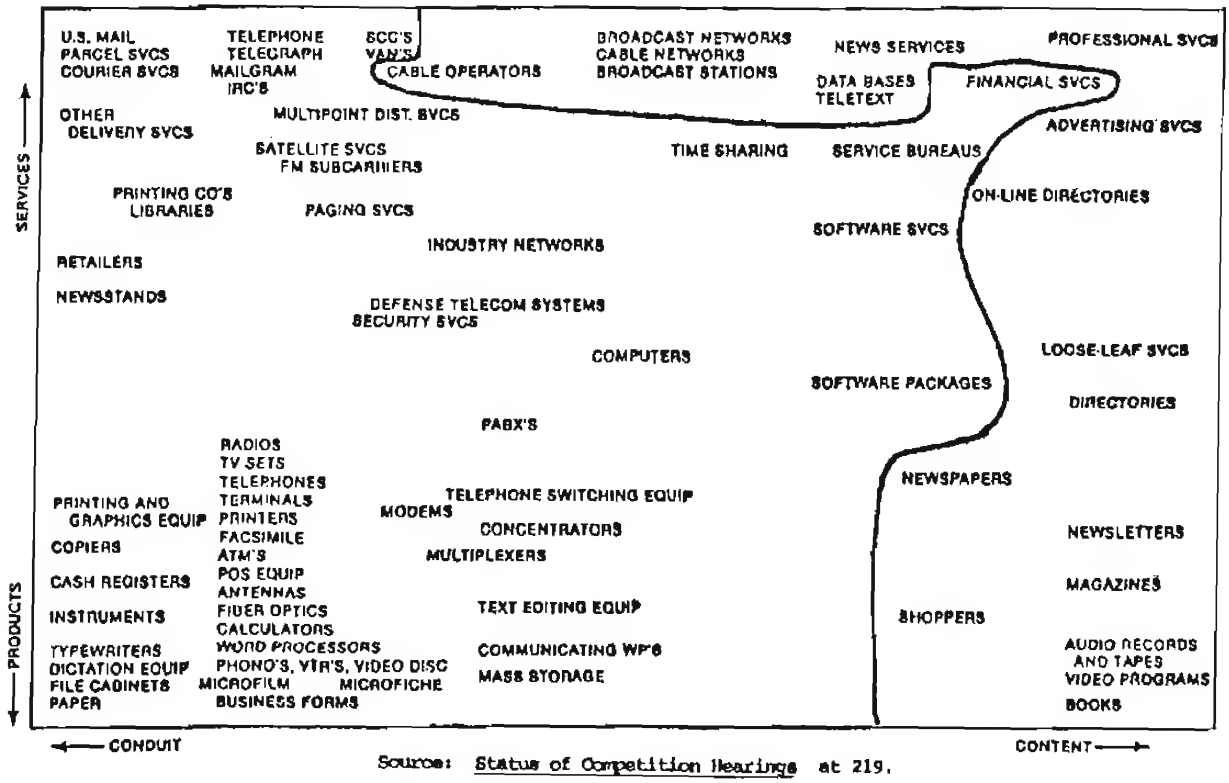
~~(S-CCO)~~ This variety and complexity would not matter directly to SIGINT were it not for the fact that as the new networks become more efficient, it will become a matter of economic necessity to supply the products and services by electronic means. The development of E-Mail, to compensate for the cost and delay of postal services, and the corresponding development of robots to answer phone calls, place calls, and telemeter building conditions--because of high labor costs, lack of servants, and a consumer market for such "personal" services--is a further illustration of the increasing use of electronics and telecoms to perform social and economic functions.

P.L. 86-36
E0 1.4.(c)

[redacted]

~~(S-CCO)~~ The "mining" of some of the teleservice transactions would be comparable to the vast diamond recovery operations off the coast of South Africa, where a bulldozers continuously work to push a sand dike farther out to sea, while huge machines dig up the exposed seafloor and screen alluvial diamonds.

THE MEDIA BUSINESSES, 1981 Fig. 37



Source: Status of Competition Hearings at 219.

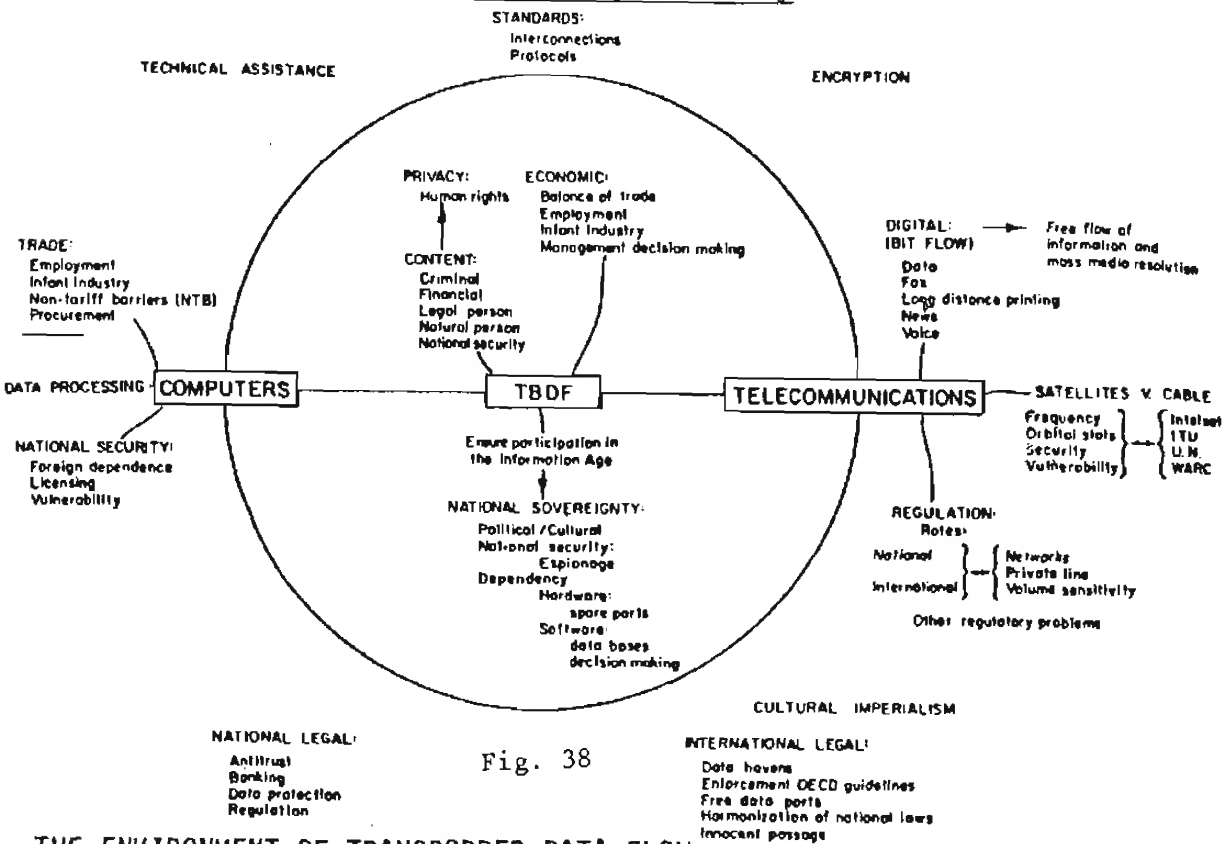


Fig. 38

THE ENVIRONMENT OF TRANSBORDER DATA FLOW

The ratio of sand moved to diamonds extracted is about 130 million to one. While some SIGINT will continue to operate against high grade teleservices such as dedicated military and diplomatic cipher links, other SIGINT will have to work the huge mass of low grade transactions, which may be coded or encrypted in a way that conceals their lack of value.

~~(C)~~ Put in different words, the teleservices will represent the actual policies of a nation, just as transactions and teleservices within a small computer net embody the net policies. In the course of analyzing the complex networks and teleservice repertoires, SIGINT will inevitably discover just what the social, economic and, in many cases, security policies of the target nation are. As policies change, teleservices will change with them, just as the U.S. imposed peacetime censorship on international radio and cable services in 1914, and many countries impose such censorship on various internal and transborder telecom services and transactions during wars and crises nowadays.

~~(C)~~ One elementary example of the significance of teleservices and transactions in defining policy and status is the power currently possessed by computer network managers to access and change passwords, access and rename and move files, change access codes, and monitor or alter the actual usage of network facilities, and even to take the network down or change the operating systems gradually or totally without much reference to the users or even to the owners of the nets. Their "privileged" terminals, plus far-reaching power to change and tamper and inspect, and to deny access or shut down, shows how teleservices define policy and power. In future, the power of the network managers will be a key index of where actual power in a target system is concentrated--always an interesting fact.

~~(S-CCO)~~ In capsule form, teleservices are the image of policy. Teletraffic is the image of operations defined by policy. SIGINT is the insight channel.

~~(S-CCO)~~ One of the most vivid illustrations of the complex intertwining of telecommunications and social policy is the issue of transborder data flow.

ENVIRONMENT OF TRANSBORDER DATA FLOW (Fig 38)

~~(S-CCO)~~ A Harvard study represented the TBDF (transborder data flow) problem in a semi-inscrutable diagram, with "encryption" apparently floating freely as an environmental factor. In fact, encryption will be one of the major issues in TBDF.

~~(S-CCO)~~ TBDF began as an endeavor in Europe to protect certain personal data which in several countries is protected by law from exploitation in bordering nations. This privacy interest gave it political power, and the discussion soon turned to the more interesting matter of controlling the power of foreign e.g., U.S., corporations by limiting the kinds of files and data they could send across borders by telecommunications. In France a small tax is levied on many kinds of data exports, not for revenue purposes, but to keep records on what is passing. The principal method for moving sensitive business files across borders has long been to fly them by courier as magnetic tape files, because this is much cheaper and more accurate for subsequent processing on U.S.-based computers. However, the European nations have begun to draft regional legislation to control all kinds of files to establish non-tariff trade barriers and other limitations on foreign companies. The Canadians have also taken a view that TBDF represents a loss of jobs in Canada.

~~(S-CCO)~~ U.S. business interests not only want "free flow of information," but also claim a "right" to operate cryptographic devices over transborder data channels. Most transborder telephone lines to and from the U.S. are leased and are used by corporations for their internal communications.

~~(S-CCO)~~ For the foreign governments to impose their TBDF policies, they must have access to the contents of the traffic passing over their borders. Under international law (The International Telecommunications Convention) they have the legal power to examine any non-government traffic that terminates in their territory. Encryption would thwart the power of the state. Therefore, encryption will be a central issue in TBDF.

~~(C)~~ Because there are many subtle ways to send traffic across borders (e.g., indirect transmission to an undeclared recipient, etc.), the PTT's and security services will have to use their own SIGINT and intelligence services to verify that the actual TBDF corresponds to their laws and policies. The U.S. is one of the most important players in the TBDF controversy, because quite a lot of technology transfer occurs from U.S. data bases to foreign subscribers, and U.S.

transnational corporations are major users of advanced data services.

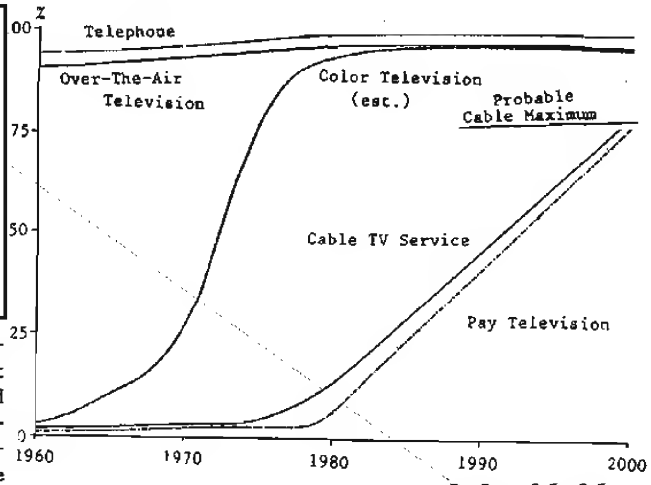
[redacted]

(U) One of the driving factors in telecommunications and teleservices which is not under the control of the telecom planners and managers, is the market penetration of consumer communications devices, such as telephones, TV sets, radios, stereos, mobile radios, home computers, etc.

(U) As the public acquires these communication devices, the PTT's and manufacturers and network designers have to develop supporting services to correspond to the consumer needs. Thus, for example, microwave radio relay stations and trunk routes spread throughout the U.S., Europe, and the rest of the world at a very high rate after World War II to provide a cheap wideband channel for distribution of TV programs. The programs were expensive to produce, compared to radio programs, and, before video tapes existed, had to be distributed from central studios. There was no security problem, so radio relay was acceptable. After the microwave trunks were installed and functioning, additional equipment was developed to carry telephone traffic. The driving factor was the success of the TV receiver in the market, which created a demand for the wideband network.

(U) Even consumer communications reflect commercial or governmental policies. In Israel only black and white programs are broadcast, to thwart sales of imported color TV sets, because the Israeli economy cannot stand the outflow of hard currency. At the same time, TV sets in Israel are only allowed to receive UHF so that the powerful Arab VHF programs cannot be heard. In the U.S. the broadcasters with good VHF frequencies have been influential in retarding the use of UHF and cable as a competing medium.

Percent Penetration in U.S. Homes



P.L. 86-36
EO 1.4.(c)

MARKET PENETRATION OF CONSUMER ELECTRONICS (Fig 39)

[redacted]

(U) A very different implication comes from the growth of pay-TV. This has been shown to be a profitable way of selling certain kinds of entertainment because the revenues are directly connected to market success of specific entertainment products. In order to keep non-paying viewers out, TV encryption systems have come into use. At present most of them are very weak and can be circumvented, but much better systems are under development. In the U.S. the pay-TV distribution consists of two parts, viz., the distribution of program material from a central point to local CATV companies, and the further distribution by local broadcasting. There is also a background of TVRO small earth stations which intercept both pay-TV and ordinary TV satellite relay transmissions.

(U) As pay-TV gains in success and is able to sell better programs, the economic value of TV encryption will increase. On the satellite links it is worth while to provide fairly secure encryption, but the emphasis is on program quality after decoding. In general the voice channel will be secured by something equivalent to DES. At the local level, quality is less important to the supplier than being able to defeat piracy and assuring that all customers pay their bills. The emphasis in encryption is on the command channel that shuts sets off if they are stolen or delinquent in payment.

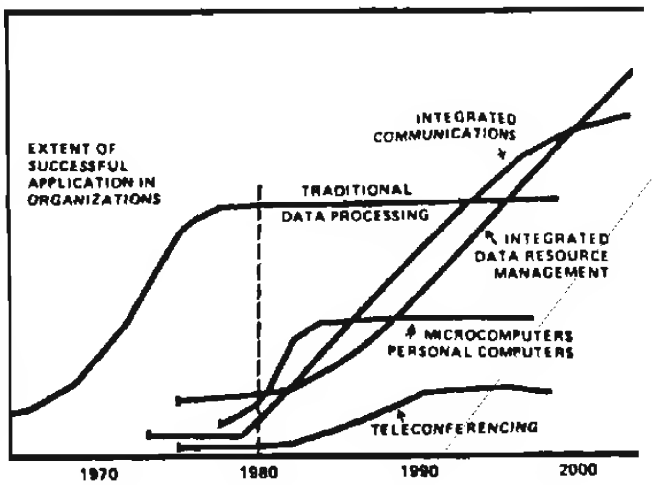
(U) The growth of many specialized TV services, including pay-TV, has made U.S. domsats (domestic satellites) a profitable industry over the past two years, and three quarters of the domsat transponders are used for TV relay.

~~(C)~~ As these new TV services, especially pay-TV, spread to foreign countries as ways of making money or raising PTT revenues, the encryption schemes will spread with them. The result will be that most of the foreign domsats will be carrying encrypted wideband traffic. The U.S. market study shows pay-TV at a 40-percent penetration level by 1990. The penetration will probably lag in most foreign countries, but the use of wideband encryption on TV satellite relays may spread faster than local TV encryption to thwart interception or copying of national programs.

~~(S-CCO)~~

(U) All of this will add to the burden on SIGINT to know what is passing through the networks, and what services are being offered, on channels which in the past have been of no interest at all.

(U) An additional implication is that the development and deployment of wideband encrypted broadcast trunks, in the U.S. or elsewhere, will have a significant strategic impact because of the difficulty of knowing the true purpose of the broadcast facilities. At the very least, it will create more international tension and suspicion unless special arrangements are made for exchange of keys on benign entertainment links. But any such exchange of keys would defeat the marketability of conference services, so that commercial interests may be directly contrary to strategic interests.



Concurrent learning curves for new technologies.

P.L. 86-36
EO 1.4.(c)

LEARNING CURVES FOR USERS (Fig 40)

(U) When a new technology or service is introduced, it does not usually reach its full development at that point. There is an S-shaped learning curve, and at the beginning progress may be quite slow. At some point the utility levels off.

(U) In service industries there are usually diseconomies of scale because internal coordination and administration increase faster than the size of the organization. One of the schemes for reducing these inefficiencies is for the high-level people, both technical and managerial, to use automatic systems, viz., terminal systems, to get their work done, without having to expend energy in human coordination and administration. Even this kind of scheme implies a long learning time, for individuals or organizations.

~~(C-CCO)~~ The implication to SIGINT is twofold. In the first place, no matter how quickly new technologies and services are introduced into target networks, it will take the target users some time to learn how to use them efficiently, or even to use them at all. Security or political limitations may slow down this learning even more. This creates a theoretical opportunity for SIGINT to pick up the target usage at an early stage, and follow

it as the users become more proficient and extend the usage. However, this creates a requirement for continuity and for slack capacity within the SIGINT system so that some response to new events is possible without tearing up all the existing operations.

[redacted]

~~(C-CCO)~~ In any service activity, the diseconomies of scale are always a peril to competitive survival. SIGINT faces the special hazards that the target telecom nets are expanding inexorably in a way that will defeat any small analytic and processing effort, while at the same time the combination of secret and unknown information, and technical complexity, will force more and more internal coordination--through the "unified integrated" centralized analytic centers. With this combination of an increasing volume of data and greater coordination and decision cost per datum, any mathematical model of the process would explode.

MAIL BOX

From: rcg at BROWN2
Subject: shell game
To: cryptolg at barlc05

Hi,

~~(C)~~ We just received a copy of the August 1982 CRYPTOLOG here at Menwith Hill Station (association with NSA is CONFIDENTIAL). I read with interest the SHELL GAME article. By the way, I think it is a good idea to maintain this kind of interchange.

P.L. 86-36

(U) I have some comments on the shell written by [redacted] to transfer files using cftp. I believe it a good idea to begin using programs which request the user account name and password when connecting to other systems. We all have too many shell files which place the login line complete with password right in the file. The newer version of UNIX (PWB), in addition to including the 'gather' program, provides some new features which may accomplish the same purpose. Specifically, the shell process now allows one to easily read input direct from the terminal. The 'pump' command, implemented within the shell, allows the user to place input parameters into command lines of a called process (like cftp), where normal shell arguments ($1,...) do not work.

P.L. 86-36
EO 1.4.(c)

(U) Also I might note the writer's problem with the line 'stty -echo > /dev/ttyX'. On any Agency UNIX system, the generic device name '/dev/tty' may always be used to specify the current terminal which is being used. Thus there is no need to worry about finding one's terminal ID to put into a shell.

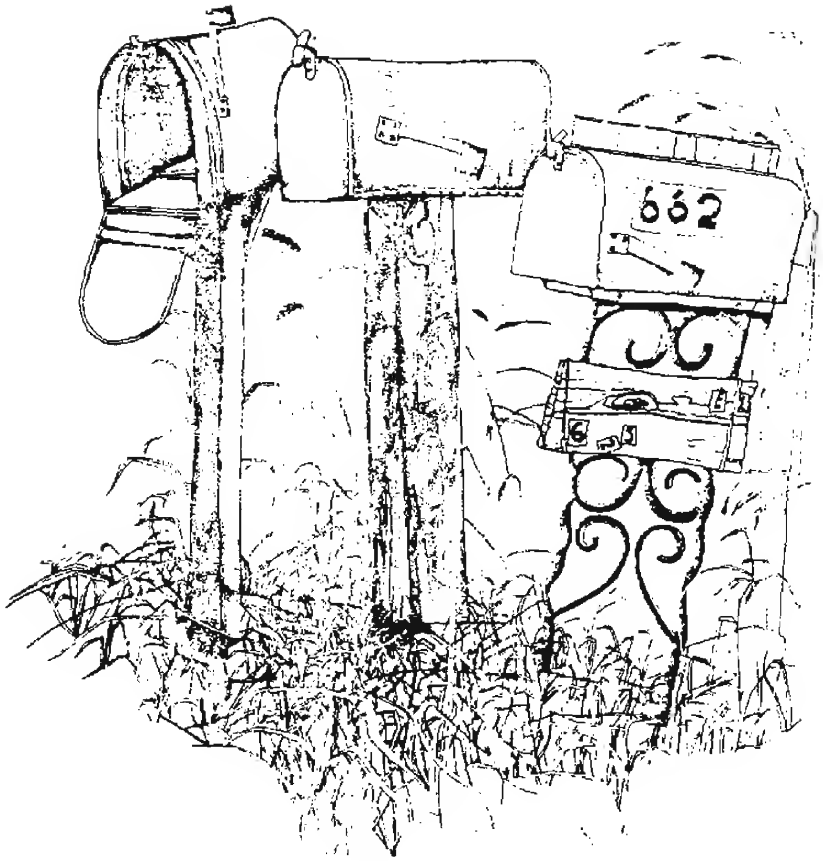
[redacted]

P.L. 86-36

SOLUTION TO NSA-CROSTIC No. 43

"[The] Uses of Elegant English," [redacted] CRYPTOLOG, November, 1976.

"It was Engelbert Humperdinck, I think, who sang a song recently, whose lyrics are the epitome of originality and poetic imagery of which today's songwriters can be so proud. 'I'm yours,' sang Mr. Humperdinck, 'till the stars fall from the sky, for you and I.'"



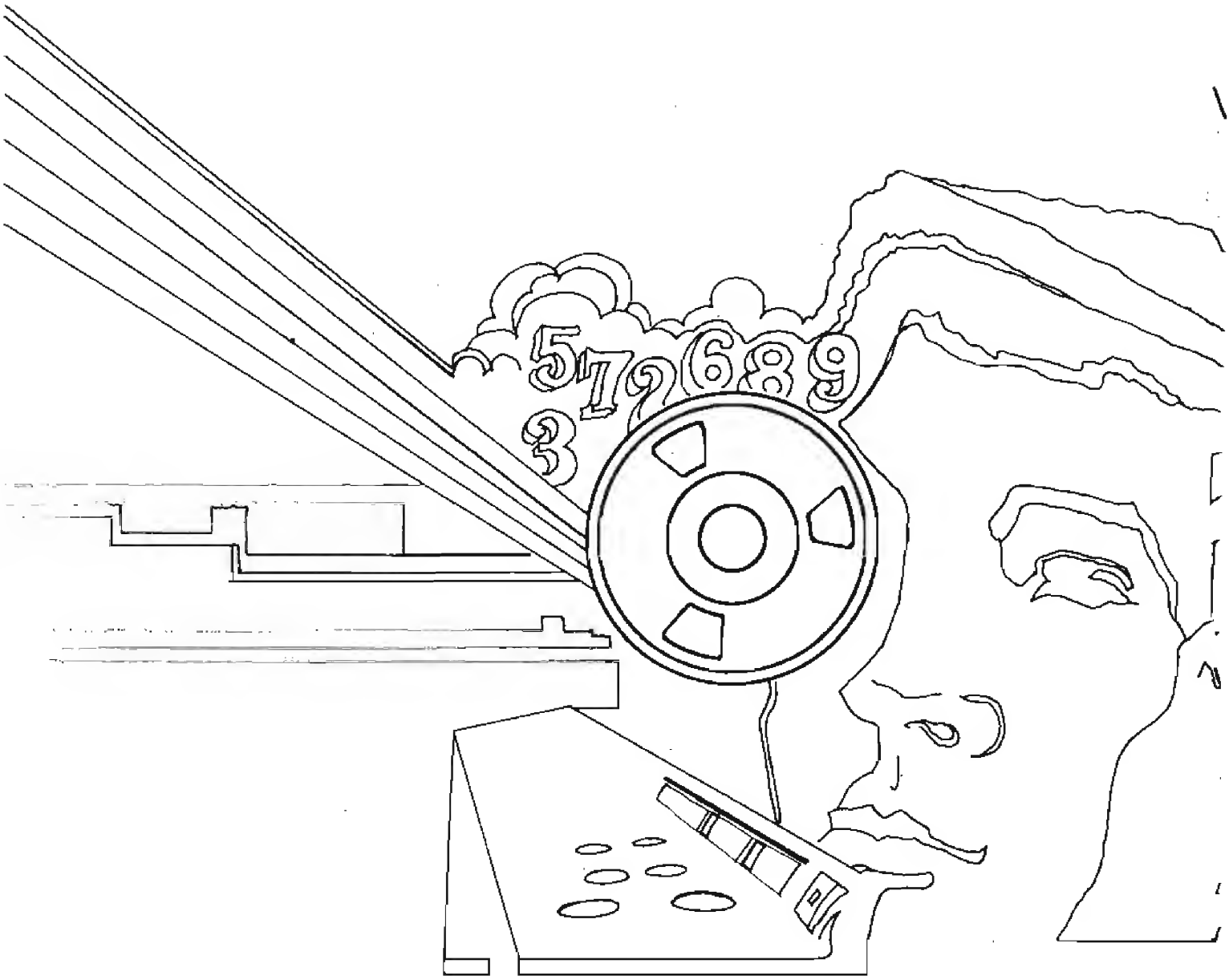
If you would like to have

CRYPTOLOG sent directly to you...

Call

[redacted] ***on x3369s.***

P.L. 86-36


5726893